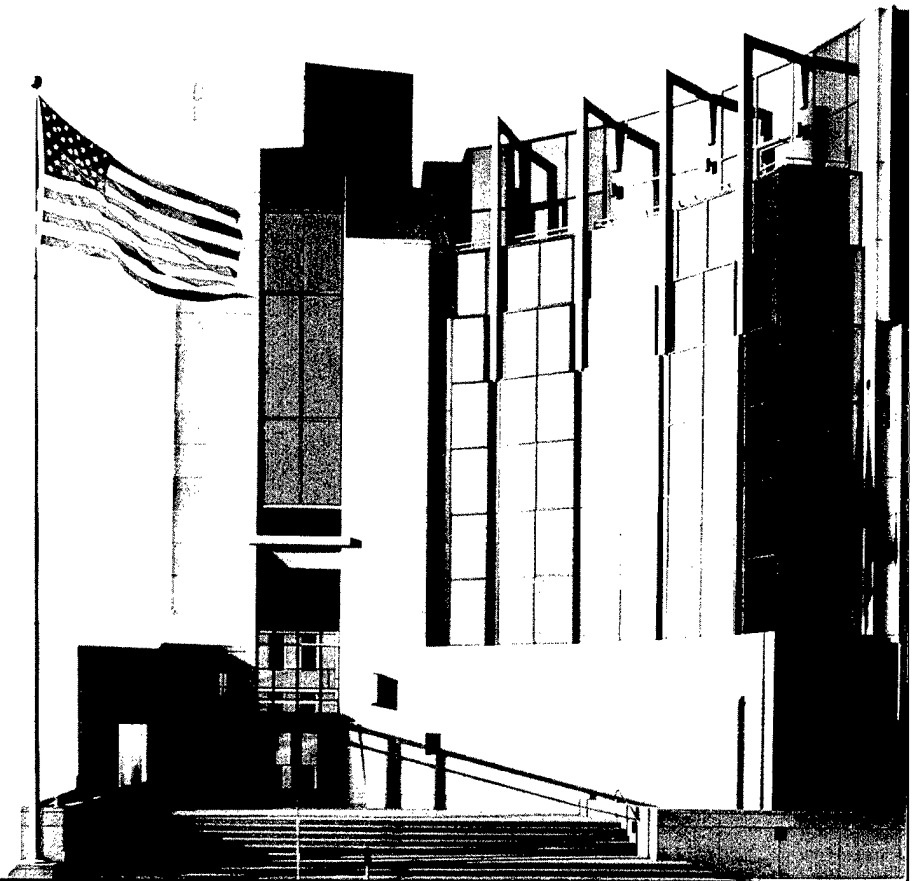
Carnegie Mellon
Software Engineering Institute

OCTAVE®-S Implementation Guide, Version 1.0

Volume 9: Strategy and Plan Worksheets

Christopher Alberts
Audrey Dorofee
James Stevens
Carol Woody

January 2005



HANDBOOK
CMU/SEI-2003-HB-003

Carnegie Mellon
Software Engineering Institute

Pittsburgh, PA 15213-3890

OCTAVE®-S Implementation Guide, Version 1.0

Volume 9: Strategy and Plan Worksheets

CMU/SEI-2003-HB-003

Christopher Alberts
Audrey Dorofee
James Stevens
Carol Woody

January 2005

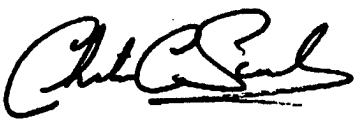
Networked Systems Survivability Program

This report was prepared for the

SEI Joint Program Office
ESC/XPK
5 Eglin Street
Hanscom AFB, MA 01731-2100

The ideas and findings in this report should not be construed as an official DoD position. It is published in the interest of scientific and technical information exchange.

FOR THE COMMANDER



Christos Scondras
Chief of Programs, XPK

This work is sponsored by the U.S. Department of Defense. The Software Engineering Institute is a federally funded research and development center sponsored by the U.S. Department of Defense.

This work was created in the performance of Federal Government Contract Number F19628-00-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013.

For information about purchasing paper copies of SEI reports, please visit the publications portion of our Web site (http://www.sei.cmu.edu/publications/pubweb.html).

Table of Contents

List of Tables

About This Document

This document is Volume 9 of the *OCTAVE-S Implementation Guide*, a 10-volume handbook supporting the OCTAVE-S methodology. This volume contains worksheets to record the organization's current and desired protection strategies and the risk mitigation plans.

The volumes in this handbook are

- *Volume 1: Introduction to OCTAVE-S* – This volume provides a basic description of OCTAVE-S and advice on how to use the guide.
- *Volume 2: Preparation Guidelines* – This volume contains background and guidance for preparing to conduct an OCTAVE-S evaluation.
- *Volume 3: Method Guidelines* – This volume includes detailed guidance for each OCTAVE-S activity.
- *Volume 4: Organizational Information Workbook* – This volume provides worksheets for all organizational-level information gathered and analyzed during OCTAVE-S.
- *Volume 5: Critical Asset Workbook for Information* – This volume provides worksheets to document data related to critical assets that are categorized as information.
- *Volume 6: Critical Asset Workbook for Systems* – This volume provides worksheets to document data related to critical assets that are categorized as systems.
- *Volume 7: Critical Asset Workbook for Applications* – This volume provides worksheets to document data related to critical assets that are categorized as applications.
- *Volume 8: Critical Asset Workbook for People* – This volume provides worksheets to document data related to critical assets that are categorized as people.
- ***Volume 9: Strategy and Plan Workbook*** – This volume provides worksheets to record the current and desired protection strategy and the risk mitigation plans.
- *Volume 10: Example Scenario* – This volume includes a detailed scenario illustrating a completed set of worksheets.

Abstract

The Operationally Critical Threat, Asset, and Vulnerability Evaluation[SM] (OCTAVE®) approach defines a risk-based strategic assessment and planning technique for security. OCTAVE is a self-directed approach, meaning that people from an organization assume responsibility for setting the organization's security strategy. OCTAVE-S is a variation of the approach tailored to the limited means and unique constraints typically found in small organizations (less than 100 people). OCTAVE-S is led by a small, interdisciplinary team (three to five people) of an organization's personnel who gather and analyze information, producing a protection strategy and mitigation plans based on the organization's unique operational security risks. To conduct OCTAVE-S effectively, the team must have broad knowledge of the organization's business and security processes, so it will be able to conduct all activities by itself.

1 Introduction

This document contains the Operationally Critical Threat, Asset, and Vulnerability[SM] (OCTAVE®)-S worksheets related to the organization's strategy development and planning activities.

Table 1 provides a brief introduction to the contents of this workbook, using activity step numbers as a key. For more details about how to complete each step, refer to the *OCTAVE®-S Method Guidelines*, which can be found in Volume 3 of the *OCTAVE®-S Implementation Guide*.

Table 1: Worksheets Provided in This Workbook

Step	Description	Worksheet	Activity	Pages
---	Document notes and recommendations identified during each step.	Notes and Recommendations	All Phases All Processes All Activities	3-12
---	Document action items identified during each step.	Action List	All Phases All Processes All Activities	13-22
Step 25	Transfer the stoplight status of each security practice area to the corresponding area of the *Protection Strategy worksheet.* For each security practice area, identify your organization's current approach for addressing that area.	Protection Strategy	Phase 3 Process S5 S5.1 Describe Current Protection Strategy	23-82

[SM] Operationally Critical Threat, Asset, and Vulnerability Evaluation is a service mark of Carnegie Mellon University.

® OCTAVE is registered in the United States Patent and Trademark Office by Carnegie Mellon University.

Table 1: Worksheets Provided in This Workbook (cont.)

Step	Description	Worksheet	Activity	Pages
Step 28	Develop mitigation plans for each security practice area selected during Step 27. As you complete this step, if you have difficulty coming up with potential mitigation activities for a security practice area, review examples of mitigation activities for that area in the *Mitigation Activities Guide*.	Mitigation Plan	Phase 3 Process S5 S5.3 Develop Risk Mitigation Plans	115-128
Step 29	Determine whether your mitigation plans affect your organization's protection strategy. Record any changes on the *Protection Strategy worksheet*. Next, review the protection strategy, including proposed changes. Determine whether you intend to make any additional changes to the protection strategy. Record any additional changes on the *Protection Strategy worksheet*.	Protection Strategy	Phase 3 Process S5 S5.4 Identify Changes to Protection Strategy	23-82
Step 30	Determine what your organization must do to implement the results of this evaluation and improve its security posture.	Next Steps	Phase 3 Process S5 S5.5 Identify Next Steps	129-132

2 Notes and Recommendations Worksheet

All Phases All Processes All Activities	
Throughout Evaluation	Document notes and recommendations identified during each step.

Note

What notes do you want to record? *Is there a recommendation associated with this note? If yes, document it in the corresponding recommendations box.*	*For which step is this note relevant?*
	Step _____

Note

What notes do you want to record? *Is there a recommendation associated with this note? If yes, document it in the corresponding recommendations box.*	*For which step is this note relevant?*
	Step _____

Recommendation

What recommendations do you want to record?	*For which step is this recommendation relevant?*
	Step _____

Recommendation

What recommendations do you want to record?	*For which step is this recommendation relevant?*
	Step _____

Note

What notes do you want to record? *Is there a recommendation associated with this note? If yes, document it in the corresponding recommendations box.*	*For which step is this note relevant?*
	Step _____

Note

What notes do you want to record? *Is there a recommendation associated with this note? If yes, document it in the corresponding recommendations box.*	*For which step is this note relevant?*
	Step _____

Recommendation	
What recommendations do you want to record?	*For which step is this recommendation relevant?*
	Step _____

Recommendation	
What recommendations do you want to record?	*For which step is this recommendation relevant?*
	Step _____

Note	
What notes do you want to record? *Is there a recommendation associated with this note? If yes, document it in the corresponding recommendations box.*	*For which step is this note relevant?*
	Step _____

Note	
What notes do you want to record? *Is there a recommendation associated with this note? If yes, document it in the corresponding recommendations box.*	*For which step is this note relevant?*
	Step _____

Recommendation

What recommendations do you want to record?	*For which step is this recommendation relevant?*
	Step _____

Recommendation

What recommendations do you want to record?	*For which step is this recommendation relevant?*
	Step _____

Note

What notes do you want to record? *Is there a recommendation associated with this note? If yes, document it in the corresponding recommendations box.*	*For which step is this note relevant?*
	Step _____

Note

What notes do you want to record? *Is there a recommendation associated with this note? If yes, document it in the corresponding recommendations box.*	*For which step is this note relevant?*
	Step _____

Recommendation

What recommendations do you want to record?	*For which step is this recommendation relevant?*
	Step _____

Recommendation

What recommendations do you want to record?	*For which step is this recommendation relevant?*
	Step _____

3 Action List Worksheet

All Phases All Processes All Activities	
Throughout Evaluation	Document action items identified during each step.

Action Item		
ID # _____	*What actions do you intend to take?* *Assign an identification number to each action item.*	*For which step is this action item relevant?* Step _____

Action Item		
ID # _____	*What actions do you intend to take?* *Assign an identification number to each action item.*	*For which step is this action item relevant?* Step _____

	Action Item
	What additional information do you want to document for each action item? *Record additional information below.*
Responsibility:	*Who is responsible for completing the action item?*
Completion Date:	*By when must the action item be completed?*
Additional Support:	*What additional support (by management or others) is required to complete the action item?*

	Action Item
	What additional information do you want to document for each action item? *Record additional information below.*
Responsibility:	*Who is responsible for completing the action item?*
Completion Date:	*By when must the action item be completed?*
Additional Support:	*What additional support (by management or others) is required to complete the action item?*

Action Item		
	What actions do you intend to take? *Assign an identification number to each action item.*	*For which step is this action item relevant?*
ID # _____		Step _____

Action Item		
	What actions do you intend to take? *Assign an identification number to each action item.*	*For which step is this action item relevant?*
ID # _____		Step _____

	Action Item
	What additional information do you want to document for each action item? *Record additional information below.*
Responsibility:	*Who is responsible for completing the action item?*
Completion Date:	*By when must the action item be completed?*
Additional Support:	*What additional support (by management or others) is required to complete the action item?*

	Action Item
	What additional information do you want to document for each action item? *Record additional information below.*
Responsibility:	*Who is responsible for completing the action item?*
Completion Date:	*By when must the action item be completed?*
Additional Support:	*What additional support (by management or others) is required to complete the action item?*

Action Item

ID #	*What actions do you intend to take?* *Assign an identification number to each action item.*	*For which step is this action item relevant?*
_____		Step _____

Action Item

ID #	*What actions do you intend to take?* *Assign an identification number to each action item.*	*For which step is this action item relevant?*
_____		Step _____

	Action Item
	What additional information do you want to document for each action item? *Record additional information below.*
Responsibility:	*Who is responsible for completing the action item?*
Completion Date:	*By when must the action item be completed?*
Additional Support:	*What additional support (by management or others) is required to complete the action item?*

	Action Item
	What additional information do you want to document for each action item? *Record additional information below.*
Responsibility:	*Who is responsible for completing the action item?*
Completion Date:	*By when must the action item be completed?*
Additional Support:	*What additional support (by management or others) is required to complete the action item?*

Action Item

ID #	*What actions do you intend to take?* *Assign an identification number to each action item.*	*For which step is this action item relevant?*
_____		Step _____

Action Item

ID #	*What actions do you intend to take?* *Assign an identification number to each action item.*	*For which step is this action item relevant?*
_____		Step _____

	Action Item
	What additional information do you want to document for each action item? *Record additional information below.*
Responsibility:	*Who is responsible for completing the action item?*
Completion Date:	*By when must the action item be completed?*
Additional Support:	*What additional support (by management or others) is required to complete the action item?*

	Action Item
	What additional information do you want to document for each action item? *Record additional information below.*
Responsibility:	*Who is responsible for completing the action item?*
Completion Date:	*By when must the action item be completed?*
Additional Support:	*What additional support (by management or others) is required to complete the action item?*

4 Protection Strategy Worksheet

Phase 3
Process S5
Activity S5.1

Step 25	Transfer the stoplight status of each security practice area to the corresponding area of the *Protection Strategy worksheet.* For each security practice area, identify your organization's current approach for addressing that area.

Phase 3
Process S5
Activity S5.4

Step 29	Determine whether your mitigation plans affect your organization's protection strategy. Record any changes on the *Protection Strategy worksheet.* Next, review the protection strategy, including proposed changes. Determine whether you intend to make any additional changes to the protection strategy. Record any additional changes on the *Protection Strategy worksheet.*

1. Security Awareness and Training

Stoplight Status ☐

Step 25: How formal is your organization's training strategy?

Step 29: Will any mitigation activities change your training strategy?
Do you want to make any additional changes to your training strategy?

Training Strategy	Step 25	Step 29
The organization has a documented training strategy that includes security awareness training and security-related training for supported technologies.	☐ Current	☐ Change
The organization has an informal and undocumented training strategy.	☐ Current	☐ Change
_____	☐ Current	☐ Change
_____		

Step 25: How often is security awareness training provided?

Step 29: Will any mitigation activities change how often security awareness training is provided?
Do you want to make any additional changes to how often security awareness training is provided?

Security Awareness Training	Step 25	Step 29
Periodic security awareness training is provided for all employees _____time(s) every _____ years.	☐ Current	☐ Change
Security awareness training is provided for new staff members as part of their orientation activities.	☐ Current	☐ Change
The organization does not provide security awareness training. Staff members learn about security issues on their own.	☐ Current	☐ Change
_____	☐ Current	☐ Change
_____		

1. Security Awareness and Training

Step 25: To what extent are IT staff members required to attend security-related training?

Step 29: Will any mitigation activities change the requirement for attending security-related training?
Do you want to make any additional changes to the requirement for attending security-related training?

Security-Related Training for Supported Technologies	Step 25	Step 29
Information technology staff members are required to attend security-related training for any technologies that they support.	❑ Current	❑ Change
Information technology staff members can attend security-related training for any technologies that they support if they request it.	❑ Current	❑ Change
The organization generally does not provide opportunities for information technology staff members to attend security-related training for supported technologies. Information technology staff members learn about security-related issues on their own.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

Step 25: How formal is your organization's mechanism for providing periodic security updates?

Step 29: Will any mitigation activities change your mechanism for providing periodic security updates?
Do you want to make any additional changes to your mechanism for providing periodic security updates?

Periodic Security Updates	Step 25	Step 29
The organization has a formal mechanism for providing staff members with periodic updates/bulletins about important security issues.	❑ Current	❑ Change
The organization does not have a mechanism for providing staff members with periodic updates/bulletins about important security issues.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

1. Security Awareness and Training

Stoplight Status ☐

Step 25: How formal is your organization's mechanism for verifying that staff receives training?

Step 29: Will any mitigation activities change your mechanism for verifying that staff receives training?
Do you want to make any additional changes to your mechanism for verifying that staff receives training?

Training Verification	Step 25	Step 29
The organization has formal mechanisms for tracking and verifying that staff members receive appropriate security-related training.	☐ Current	☐ Change
The organization has informal mechanisms for tracking and verifying that staff members receive appropriate security-related training.	☐ Current	☐ Change
The organization has no mechanisms for tracking and verifying that staff members receive appropriate security-related training.	☐ Current	☐ Change
_____	☐ Current	☐ Change
_____		

Step 25: What additional characteristic of your current approach to security awareness and training do you want to record?

Step 29: Will any mitigation activities change this characteristic?
Do you want to make any additional changes to this characteristic?

Other:	Step 25	Step 29
_____	☐ Current	☐ Change
_____		
_____	☐ Current	☐ Change
_____		
_____	☐ Current	☐ Change
_____		

2. Security Strategy

Stoplight Status ☐

Step 25: How formal is your organization's mechanism for integrating security and business strategies?

Step 29: Will any mitigation activities change your mechanism for integrating security and business strategies? Do you want to make any additional changes to your mechanism for integrating security and business strategies?

Business and Security Strategy Integration	Step 25	Step 29
The organization has formal mechanisms for integrating • security considerations into business strategies • business strategies and goals into security strategies and policies	☐ Current	☐ Change
The organization has informal mechanisms for integrating • security considerations into business strategies • business strategies and goals into security strategies and policies	☐ Current	☐ Change
The organization has no mechanisms for integrating • security considerations into business strategies • business strategies and goals into security strategies and policies	☐ Current	☐ Change
_____ _____	☐ Current	☐ Change

Step 25: How formal are your organization's security strategies, goals, and objectives?

Step 29: Will any mitigation activities change your security strategies, goals, and objectives? Do you want to make any additional changes to your security strategies, goals, and objectives?

Documented Strategies	Step 25	Step 29
The organization has documented security strategies, goals, and objectives.	☐ Current	☐ Change
The organization has a partial set of documented security strategies, goals, and objectives. Some aspects of security strategies, goals, and objectives are informal and undocumented.	☐ Current	☐ Change
The organization has informal and undocumented security strategies, goals, and objectives.	☐ Current	☐ Change
_____ _____	☐ Current	☐ Change

2. Security Strategy

Step 25: To what extent does your security awareness training program include information about the organization's security strategy?

Step 29: Will any mitigation activities change the content of your security awareness training to include strategy information?
Do you want to make any additional changes to the content of your security awareness training?

Staff Awareness	Step 25	Step 29
The organization's security awareness training program includes information about the organization's security strategy. This training is provided for all employees _____time(s) every _____ years.	❑ Current	❑ Change
The organization's security awareness training program includes information about the organization's security strategy. This training is provided for new staff members as part of their orientation activities.	❑ Current	❑ Change
The organization's security awareness training program does not include information about the organization's security strategy. Staff members learn about the organization's security strategy on their own.	❑ Current	❑ Change
_____	❑ Current	❑ Change

Step 25: What additional characteristic of your current approach to security strategy do you want to record?

Step 29: Will any mitigation activities change this characteristic?
Do you want to make any additional changes to this characteristic?

Other:	Step 25	Step 29
_____	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____	❑ Current	❑ Change

3. Security Management

Stoplight Status ☐

Step 25: To what extent are security roles and responsibilities formally defined?

Step 29: Will any mitigation activities change the extent to which security roles and responsibilities are formally defined? Do you want to make any additional changes to how security roles and responsibilities are formally defined?

Roles and Responsibilities	Step 25	Step 29
The organization has formally documented information security roles and responsibilities for all staff in the organization.	❑ Current	❑ Change
The organization has formally documented information security roles and responsibilities for selected staff in the organization.	❑ Current	❑ Change
The organization has informal and undocumented information security roles and responsibilities.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

Step 25: To what extent is security formally factored into your organization's budget?

Step 29: Will any mitigation activities change how security is formally factored into your organization's budget? Do you want to make any additional changes to how security is formally factored into your organization's budget?

Funding	Step 25	Step 29
The organization's budget has a distinct line item for information security activities. The funding level is determined based on a formal assessment of the organization's information security risks.	❑ Current	❑ Change
The organization's budget has a distinct line item for information security activities. The funding level is determined using informal processes.	❑ Current	❑ Change
The organization's budget explicitly includes information security activities under the line item for information technology (IT). The funding level is determined based on a formal assessment of the organization's information security risks.	❑ Current	❑ Change
The organization's budget explicitly includes information security activities under the line item for information technology. The funding level is determined using informal processes.	❑ Current	❑ Change
Neither the organization's budget nor the IT department's budget explicitly includes funding for information security activities.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

3. Security Management

Step 25: How formal are your organization's security-related human resource procedures?

Step 29: Will any mitigation activities change your security-related human resource procedures? Do you want to make any additional changes to your security-related human resource procedures?

Human Resource Procedures	Step 25	Step 29
The organization has formally defined procedures for including security considerations in the organization's hiring (e.g., background checks) and termination (e.g., removing access to all systems and information) processes.	❑ Current	❑ Change
The organization has some formally defined procedures for including security considerations in the organization's hiring (e.g., background checks) and termination (e.g., removing access to all systems and information) processes. Some procedures in this area are informal and undocumented.	❑ Current	❑ Change
The organization has informal and undocumented procedures for including security considerations in the organization's hiring (e.g., background checks) and termination (e.g., removing access to all systems and information) processes.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

Step 25: How formal is your organization's process for managing information security risk?

Step 29: Will any mitigation activities change your process for managing information security risk? Do you want to make any additional changes to your process for managing information security risk?

Risk Management	Step 25	Step 29
The organization has a formally defined process for assessing and managing its information security risks.	❑ Current	❑ Change
The organization has a formally defined process for assessing its information security risks. The process for managing information security risks is informal and undocumented.	❑ Current	❑ Change
The organization has an informal and undocumented approach for assessing and managing its information security risks.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

3. Security Management

Stoplight Status ☐

Step 25: To what extent does your security-awareness training program include information about the organization's security management process?

Step 29: Will any mitigation activities change the content of your security awareness training to include security management information?
Do you want to make any additional changes to the content of your security awareness training?

Staff Awareness	Step 25	Step 29
The organization's security-awareness training program includes information about the organization's security management process. This training is provided for all employees _____time(s) every _____ years.	☐ Current	☐ Change
The organization's security-awareness training program includes information about the organization's security management process. This training is provided for new staff members as part of their orientation activities.	☐ Current	☐ Change
The organization's security-awareness training program does not include information about the organization's security management process. Staff members learn about security management on their own.	☐ Current	☐ Change
_____	☐ Current	☐ Change
_____		

Step 25: How formal is your organization's mechanism for providing managers with security-related information?

Step 29: Will any mitigation activities change how security-related information is provided to managers?
Do you want to make any additional changes to how security-related information is provided to managers?

Management Awareness	Step 25	Step 29
The organization has a formal mechanism for providing managers with summaries of important security-related information.	☐ Current	☐ Change
The organization has an informal and undocumented mechanism for providing managers with summaries of important security-related information.	☐ Current	☐ Change
The organization has no mechanism for providing managers with summaries of important security-related information.	☐ Current	☐ Change
_____	☐ Current	☐ Change
_____		

3. Security Management

Step 25: What additional characteristic of your current approach to security management do you want to record?

Step 29: Will any mitigation activities change this characteristic?
Do you want to make any additional changes to this characteristic?

Other:	Step 25	Step 29
_____	❑ Current	❑ Change
_____		
_____	❑ Current	❑ Change
_____		
_____	❑ Current	❑ Change
_____		

4. Security Policies and Regulations

Stoplight Status ☐

Step 25: To what extent are your organization's security-related policies formally documented?

Step 29: Will any mitigation activities change the extent to which your security-related policies are formally documented? Do you want to make any additional changes to the formality and documentation of your security-related policies?

Documented Policies	Step 25	Step 29
The organization has a comprehensive set of formally documented security-related policies.	☐ Current	☐ Change
The organization has a partial set of formally documented security-related policies. Some security-related policies are informal and undocumented.	☐ Current	☐ Change
The organization's security-related policies are informal and undocumented.	☐ Current	☐ Change
_____	☐ Current	☐ Change
_____		

Step 25: How formal is your organization's mechanism for creating and updating its security-related policies?

Step 29: Will any mitigation activities change how security-related policies are created and updated? Do you want to make any additional changes to how security-related policies are created and updated?

Policy Management	Step 25	Step 29
The organization has a formal mechanism for creating and updating its security-related policies.	☐ Current	☐ Change
The organization has a formal mechanism for creating its security-related policies. The organization has an informal and undocumented mechanism for updating its security-related policies.	☐ Current	☐ Change
The organization has an informal and undocumented mechanism for creating and updating its security-related policies.	☐ Current	☐ Change
_____	☐ Current	☐ Change
_____		

4. Security Policies and Regulations

Step 25: How formal are your organization's procedures for enforcing its security-related policies?

Step 29: Will any mitigation activities change how security-related policies are enforced?
Do you want to make any additional changes to how security-related policies are enforced?

Policy Enforcement	Step 25	Step 29
The organization has formal procedures for enforcing its security-related policies. Enforcement procedures are consistently followed.	❑ Current	❑ Change
The organization has formal procedures for enforcing its security-related policies. Enforcement procedures are inconsistently followed.	❑ Current	❑ Change
The organization has informal and undocumented procedures for enforcing its security-related policies.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

Step 25: To what extent does your security-awareness training program include information about the organization's security policies and regulations?

Step 29: Will any mitigation activities change the content of your security awareness training to include security policy and regulation information?
Do you want to make any additional changes to the content of your security awareness training?

Staff Awareness	Step 25	Step 29
The organization's security-awareness training program includes information about the organization's security policies and regulations. This training is provided for all employees _____time(s) every _____ years.	❑ Current	❑ Change
The organization's security-awareness training program includes information about the organization's security policies and regulations. This training is provided for new staff members as part of their orientation activities.	❑ Current	❑ Change
The organization's security-awareness training program does not include information about the organization's security policies and regulations. Staff members learn about security policies and regulations on their own.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

4. Security Policies and Regulations

Stoplight Status ☐

Step 25: How formal are your organization's procedures for complying with security-related policies and regulations?

Step 29: Will any mitigation activities change how your organization complies with security-related policies and regulations?
Do you want to make any additional changes to how your organization complies with security-related policies and regulations?

Policy and Regulation Compliance	Step 25	Step 29
The organization has formal procedures for complying with information security policies, applicable laws and regulations, and insurance requirements.	☐ Current	☐ Change
The organization has formal procedures for complying with certain information security policies, applicable laws and regulations, and insurance requirements. Some procedures in this area are informal and undocumented.	☐ Current	☐ Change
The organization has informal and undocumented procedures for complying with information security policies, applicable laws and regulations, and insurance requirements.	☐ Current	☐ Change
_____	☐ Current	☐ Change
_____		

Step 25: What additional characteristic of your current approach to security policies and regulations do you want to record?

Step 29: Will any mitigation activities change this characteristic?
Do you want to make any additional changes to this characteristic?

Other:	Step 25	Step 29
_____	☐ Current	☐ Change
_____		
_____	☐ Current	☐ Change
_____		
_____	☐ Current	☐ Change
_____		

5. Collaborative Security Management

Stoplight Status ☐

*Step 25: How formal are your organization's policies and procedures for protecting information when working with **collaborators and partners**?*

Step 29: Will any mitigation activities change the policies and procedures for protecting information when working with collaborators and partners?
Do you want to make any additional changes to the policies and procedures for protecting information when working with collaborators and partners?

Collaborators and Partners	Step 25	Step 29
The organization has documented policies and procedures for protecting information when working with collaborators and partners.	☐ Current	☐ Change
The organization has documented policies and procedures for protecting certain information when working with collaborators and partners. The organization has informal and undocumented policies and procedures for protecting other types of information when working with collaborators and partners.	☐ Current	☐ Change
The organization has informal and undocumented policies and procedures for protecting information when working with collaborators and partners.	☐ Current	☐ Change
_____	☐ Current	☐ Change
_____		

*Step 25: How formal are your organization's policies and procedures for protecting information when working with **contractors and subcontractors**?*

Step 29: Will any mitigation activities change the policies and procedures for protecting information when working with contractors and subcontractors?
Do you want to make any additional changes to the policies and procedures for protecting information when working with contractors and subcontractors?

Contractors and Subcontractors	Step 25	Step 29
The organization has documented policies and procedures for protecting information when working with contractors and subcontractors.	☐ Current	☐ Change
The organization has documented policies and procedures for protecting certain information when working with contractors and subcontractors. The organization has informal and undocumented policies and procedures for protecting other types of information when working with contractors and subcontractors.	☐ Current	☐ Change
The organization has informal and undocumented policies and procedures for protecting information when working with contractors and subcontractors.	☐ Current	☐ Change
_____	☐ Current	☐ Change
_____		

5. Collaborative Security Management

Step 25: How formal are your organization's policies and procedures for protecting information when working with ***service providers****?*

Step 29: Will any mitigation activities change the policies and procedures for protecting information when working with service providers?
Do you want to make any additional changes to the policies and procedures for protecting information when working with service providers?

Service Providers	Step 25	Step 29
The organization has documented policies and procedures for protecting information when working with service providers.	❑ Current	❑ Change
The organization has documented policies and procedures for protecting certain information when working with service providers. The organization has informal and undocumented policies and procedures for protecting other types of information when working with service providers.	❑ Current	❑ Change
The organization has informal and undocumented policies and procedures for protecting information when working with service providers.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

Step 25: To what extent does your organization formally communicate its information protection requirements to third parties?

Step 29: Will any mitigation activities change how your organization communicates its information protection requirements to third parties?
Do you want to make any additional changes to how your organization communicates its information protection requirements to third parties?

Requirements	Step 25	Step 29
The organization documents information protection requirements and explicitly communicates them to all appropriate third parties.	❑ Current	❑ Change
The organization informally communicates information protection requirements to all appropriate third parties.	❑ Current	❑ Change
The organization does not communicate information protection requirements to third parties.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

5. Collaborative Security Management

Stoplight Status ☐

Step 25: To what extent does your organization verify that third parties are addressing information protection requirements?

Step 29: Will any mitigation activities change verification mechanisms?
Do you want to make any additional changes to verification mechanisms?

Verification	Step 25	Step 29
The organization has formal mechanisms for verifying that all third-party organizations, outsourced security services, mechanisms, and technologies meet its needs and requirements.	☐ Current	☐ Change
The organization has informal mechanisms for verifying that all third-party organizations, outsourced security services, mechanisms, and technologies meet its needs and requirements.	☐ Current	☐ Change
The organization has no mechanisms for verifying that all third-party organizations, outsourced security services, mechanisms, and technologies meet its needs and requirements.	☐ Current	☐ Change
_____	☐ Current	☐ Change
_____		

Step 25: To what extent does your security-awareness training program include information about collaborative security management?

Step 29: Will any mitigation activities change the content of your security awareness training to include information about collaborative security management?
Do you want to make any additional changes to the content of your security awareness training?

Staff Awareness	Step 25	Step 29
The organization's security-awareness training program includes information about the organization's collaborative security management policies and procedures. This training is provided for all employees _____time(s) every _____ years.	☐ Current	☐ Change
The organization's security-awareness training program includes information about the organization's collaborative security management policies and procedures. This training is provided for new staff members as part of their orientation activities.	☐ Current	☐ Change
The organization's security-awareness training program does not include information about the organization's collaborative security management policies and procedures. Staff members learn about collaborative security management policies and procedures on their own.	☐ Current	☐ Change
_____	☐ Current	☐ Change
_____		

5. Collaborative Security Management

Step 25: What additional characteristic of your current approach to collaborative security management do you want to record?

Step 29: Will any mitigation activities change this characteristic?
Do you want to make any additional changes to this characteristic?

Other:	Step 25	Step 29
_____	❑ Current	❑ Change
_____		
_____	❑ Current	❑ Change
_____		
_____	❑ Current	❑ Change
_____		

6. Contingency Planning/Disaster Recovery

Stoplight Status ☐

Step 25: To what extent has an analysis of operations, applications, and data criticality been performed?

Step 29: Will any mitigation activities change the extent to which business operations are analyzed? Do you want to make any additional changes to business operations analysis?

Business Operations Analysis	Step 25	Step 29
An analysis of operations, applications, and data criticality has been performed.	☐ Current	☐ Change
A partial analysis of operations, applications, and data criticality has been performed.	☐ Current	☐ Change
An analysis of operations, applications, and data criticality has not been performed.	☐ Current	☐ Change
_____	☐ Current	☐ Change
_____		

Step 25: To what extent has your organization documented its contingency plans?

Step 29: Will any mitigation activities change how contingency plans are documented? Do you want to make any additional changes to contingency plan documentation?

Documented Plans	Step 25	Step 29
The organization has documented business continuity or emergency operation plans, disaster recovery plan(s), and contingency plan(s) for responding to emergencies.	☐ Current	☐ Change
The organization has partially documented business continuity or emergency operation plans, disaster recovery plan(s), and contingency plan(s) for responding to emergencies. Some aspects of the plans are informal and undocumented.	☐ Current	☐ Change
The organization has informal and undocumented business continuity or emergency operation plans, disaster recovery plan(s), and contingency plan(s) for responding to emergencies.	☐ Current	☐ Change
_____	☐ Current	☐ Change
_____		

6. Contingency Planning/Disaster Recovery

Step 25: To what extent has your organization tested its contingency plans?

Step 29: Will any mitigation activities change how contingency plans are tested?
Do you want to make any additional changes to contingency plan testing?

Tested Plans	Step 25	Step 29
The organization has formally tested its business continuity or emergency operation plans, disaster recovery plan(s), and contingency plan(s) for responding to emergencies.	❑ Current	❑ Change
The organization has informally tested its business continuity or emergency operation plans, disaster recovery plan(s), and contingency plan(s) for responding to emergencies.	❑ Current	❑ Change
The organization has not tested its business continuity or emergency operation plans, disaster recovery plan(s), and contingency plan(s) for responding to emergencies.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

Step 25: To what extent is physical and electronic access to critical information formally factored into contingency plans?

Step 29: Will any mitigation activities change the extent to which information access is formally factored into contingency plans?
Do you want to make any additional changes to how information access is formally factored into contingency plans?

Information Access	Step 25	Step 29
Physical and electronic access to critical information is formally factored into the organization's contingency, disaster recovery, and business continuity plans.	❑ Current	❑ Change
Physical and electronic access to some critical information is formally factored into the organization's contingency, disaster recovery, and business continuity plans. Other types of critical information are not formally factored into the plans.	❑ Current	❑ Change
Physical and electronic access to critical information is not formally factored into the organization's contingency, disaster recovery, and business continuity plans.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

6. Contingency Planning/Disaster Recovery

Stoplight Status ☐

Step 25: To what extent does your security-awareness training program include information about contingency planning and disaster recovery?

Step 29: Will any mitigation activities change the content of your security awareness training to include information about contingency planning and disaster recovery?
Do you want to make any additional changes to the content of your security awareness training?

Staff Awareness	Step 25	Step 29
The organization's security-awareness training program includes information about the organization's contingency, disaster recovery, and business continuity plans. This training is provided for all employees _____time(s) every _____ years.	❑ Current	❑ Change
The organization's security-awareness training program includes information about the organization's contingency, disaster recovery, and business continuity plans. This training is provided for new staff members as part of their orientation activities.	❑ Current	❑ Change
The organization's security-awareness training program does not include information about the organization's contingency, disaster recovery, and business continuity plans. Staff members learn about contingency, disaster recovery, and business continuity plans on their own.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

Step 25: What additional characteristic of your current approach to contingency planning and disaster recovery do you want to record?

Step 29: Will any mitigation activities change this characteristic?
Do you want to make any additional changes to this characteristic?

Other:	Step 25	Step 29
_____	❑ Current	❑ Change
_____		
_____	❑ Current	❑ Change
_____		
_____	❑ Current	❑ Change
_____		

7. Physical Access Control

Stoplight Status ☐

Step 25: Who is currently responsible for physical access control?

Step 29: Will any mitigation activities change responsibility for physical access control?
Do you want to make any additional changes affecting responsibility for physical access control?

Responsibility	Step 25			Step 29		
	☐ Current			☐ Change		
Task	Internal	External	Combined	Internal	External	Combined
Controlling physical access to the building and premises (e.g., controlling visitor access)	☐	☐	☐	☐	☐	☐
Controlling physical access to work areas (e.g., controlling staff and visitor access)	☐	☐	☐	☐	☐	☐
Controlling physical access to IT hardware	☐	☐	☐	☐	☐	☐
Controlling physical access to software media	☐	☐	☐	☐	☐	☐
_____	☐	☐	☐	☐	☐	☐
_____	☐	☐	☐	☐	☐	☐
_____	☐	☐	☐	☐	☐	☐
_____	☐	☐	☐	☐	☐	☐
_____	☐	☐	☐	☐	☐	☐
_____	☐	☐	☐	☐	☐	☐

7. Physical Access Control

Step 25: To what extent are procedures for this area formally documented?

Step 29: Will any mitigation activities change the extent to which procedures are formally documented for this area? Do you want to make any additional changes to how procedures are documented for this area?

Procedures	Step 25	Step 29
If staff from your organization is partly or completely responsible for this area:		
The organization has formally documented plans and procedures for controlling physical access to the building and premises, work areas, IT hardware, and software media.	❑ Current	❑ Change
The organization has some formally documented policies and procedures for controlling physical access to the building and premises, work areas, IT hardware, and software media. Some policies and procedures in this area are informal and undocumented.	❑ Current	❑ Change
The organization has informal and undocumented plans and procedures for controlling physical access to the building and premises, work areas, IT hardware, and software media.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

Step 25: To what extent are staff members required to attend training in this area?

Step 29: Will any mitigation activities change the requirement for attending training in this area? Do you want to make any additional changes to the requirement for attending training in this area?

Training	Step 25	Step 29
If staff from your organization is partly or completely responsible for this area:		
Designated staff members are required to attend training that includes a review of the organization's plans and procedures for physical access control.	❑ Current	❑ Change
Designated staff members can attend training that includes a review of the organization's plans and procedures for physical access control if they request it.	❑ Current	❑ Change
The organization generally does not provide opportunities for designated staff members to attend training that includes a review of the organization's plans and procedures for physical access control. Designated staff members learn about physical access control on their own.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

7. Physical Access Control

Stoplight Status ☐

Third Party A:_____

Step 25: To what extent does your organization formally communicate its requirements in this area to this third party?

Step 29: Will any mitigation activities change how your organization communicates its requirements to this third party? Do you want to make any additional changes to how you communicate requirements to this third party?

Collaborative Issues	Step 25	Step 29
If staff from a third party is partly or completely responsible for this area:		
The organization's requirements for physical access control are formally communicated to all contractors and service providers that control physical access to the building and premises, work areas, IT hardware, and software media.	☐ Current	☐ Change
The organization's requirements for physical access control are informally communicated to all contractors and service providers that control physical access to the building and premises, work areas, IT hardware, and software media.	☐ Current	☐ Change
The organization's requirements for physical access control are not communicated to all contractors and service providers that control physical access to the building and premises, work areas, IT hardware, and software media.	☐ Current	☐ Change
_____	☐ Current	☐ Change
_____		

Step 25: To what extent does your organization verify that this third party is addressing requirements in this area?

Step 29: Will any mitigation activities change how you verify that this third party is addressing requirements in this area? Do you want to make any additional changes to how you verify that requirements are being met?

Verification	Step 25	Step 29
If staff from a third party is partly or completely responsible for this area:		
The organization formally verifies that contractors and service providers have met the requirements for physical access control.	☐ Current	☐ Change
The organization informally verifies that contractors and service providers have met the requirements for physical access control.	☐ Current	☐ Change
The organization does not verify that contractors and service providers have met the requirements for physical access control.	☐ Current	☐ Change
_____	☐ Current	☐ Change
_____		

7. Physical Access Control

Third Party B:_____

Step 25: To what extent does your organization formally communicate its requirements in this area to this third party?

Step 29: Will any mitigation activities change how your organization communicates its requirements to this third party? Do you want to make any additional changes to how you communicate requirements to this third party?

Collaborative Issues	Step 25	Step 29
If staff from a third party is partly or completely responsible for this area:		
The organization's requirements for physical access control are formally communicated to all contractors and service providers that control physical access to the building and premises, work areas, IT hardware, and software media.	❑ Current	❑ Change
The organization's requirements for physical access control are informally communicated to all contractors and service providers that control physical access to the building and premises, work areas, IT hardware, and software media.	❑ Current	❑ Change
The organization's requirements for physical access control are not communicated to all contractors and service providers that control physical access to the building and premises, work areas, IT hardware, and software media.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

Step 25: To what extent does your organization verify that this third party is addressing requirements in this area?

Step 29: Will any mitigation activities change how you verify that this third party is addressing requirements in this area? Do you want to make any additional changes to how you verify that requirements are being met?

Verification	Step 25	Step 29
If staff from a third party is partly or completely responsible for this area:		
The organization formally verifies that contractors and service providers have met the requirements for physical access control.	❑ Current	❑ Change
The organization informally verifies that contractors and service providers have met the requirements for physical access control.	❑ Current	❑ Change
The organization does not verify that contractors and service providers have met the requirements for physical access control.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

8. Monitoring and Auditing Physical Security

Stoplight Status ☐

Step 25: Who is currently responsible for monitoring and auditing physical security?

Step 29: Will any mitigation activities change responsibility for monitoring and auditing physical security? Do you want to make any additional changes affecting responsibility for monitoring and auditing physical security?

Responsibility	**Step 25**			**Step 29**		
	☐ Current			☐ Change		
Task	Internal	External	Combined	Internal	External	Combined
Keeping maintenance records to document repairs and modifications to IT hardware	☐	☐	☐	☐	☐	☐
Monitoring physical access to controlled IT hardware	☐	☐	☐	☐	☐	☐
Monitoring physical access to controlled IT software media	☐	☐	☐	☐	☐	☐
Monitoring physical access to restricted work areas	☐	☐	☐	☐	☐	☐
Reviewing monitoring records on a periodic basis	☐	☐	☐	☐	☐	☐
Investigating and addressing any unusual activity that is identified	☐	☐	☐	☐	☐	☐
_____	☐	☐	☐	☐	☐	☐
_____	☐	☐	☐	☐	☐	☐
_____	☐	☐	☐	☐	☐	☐
_____	☐	☐	☐	☐	☐	☐

8. Monitoring and Auditing Physical Security

Step 25: To what extent are procedures for this area formally documented?

Step 29: Will any mitigation activities change the extent to which procedures are formally documented for this area? Do you want to make any additional changes to how procedures are documented for this area?

Procedures	Step 25	Step 29
If staff from your organization is partly or completely responsible for this area:		
The organization has formally documented plans and procedures for monitoring physical access to the building and premises, work areas, IT hardware, and software media.	❑ Current	❑ Change
The organization has some formally documented policies and procedures for monitoring physical access to the building and premises, work areas, IT hardware, and software media. Some policies and procedures in this area are informal and undocumented.	❑ Current	❑ Change
The organization has informal and undocumented plans and procedures for monitoring physical access to the building and premises, work areas, IT hardware, and software media.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

Step 25: To what extent are staff members required to attend training in this area?

Step 29: Will any mitigation activities change the requirement for attending training in this area? Do you want to make any additional changes to the requirement for attending training in this area?

Training	Step 25	Step 29
If staff from your organization is partly or completely responsible for this area:		
Designated staff members are required to attend training for monitoring physical access to the building and premises, work areas, IT hardware, and software media.	❑ Current	❑ Change
Designated staff members can attend training for monitoring physical access to the building and premises, work areas, IT hardware, and software media if they request it.	❑ Current	❑ Change
The organization generally does not provide opportunities for designated staff members to attend training for monitoring physical access to the building and premises, work areas, IT hardware, and software media. Designated staff members learn about monitoring physical access on their own.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

8. Monitoring and Auditing Physical Security

Stoplight Status ☐

Third Party A: _____

Step 25: To what extent does your organization formally communicate its requirements in this area to this third party?

Step 29: Will any mitigation activities change how your organization communicates its requirements to this third party? Do you want to make any additional changes to how you communicate requirements to this third party?

Collaborative Issues	Step 25	Step 29
If staff from a third party is partly or completely responsible for this area:		
The organization's requirements for monitoring physical security are formally communicated to all contractors and service providers that monitor physical access to the building and premises, work areas, IT hardware, and software media.	☐ Current	☐ Change
The organization's requirements for monitoring physical security are informally communicated to all contractors and service providers that monitor physical access to the building and premises, work areas, IT hardware, and software media.	☐ Current	☐ Change
The organization's requirements for monitoring physical security are not communicated to all contractors and service providers that monitor physical access to the building and premises, work areas, IT hardware, and software media.	☐ Current	☐ Change
_____	☐ Current	☐ Change
_____		

Step 25: To what extent does your organization verify that this third party is addressing requirements in this area?

Step 29: Will any mitigation activities change how you verify that this third party is addressing requirements in this area? Do you want to make any additional changes to how you verify that requirements are being met?

Verification	Step 25	Step 29
If staff from a third party is partly or completely responsible for this area:		
The organization formally verifies that contractors and service providers have met the requirements for monitoring physical security.	☐ Current	☐ Change
The organization informally verifies that contractors and service providers have met the requirements for monitoring physical security.	☐ Current	☐ Change
The organization does not verify that contractors and service providers have met the requirements for monitoring physical security.	☐ Current	☐ Change
_____	☐ Current	☐ Change
_____		

8. Monitoring and Auditing Physical Security

Third Party B:_____

Step 25: To what extent does your organization formally communicate its requirements in this area to this third party?

Step 29: Will any mitigation activities change how your organization communicates its requirements to this third party? Do you want to make any additional changes to how you communicate requirements to this third party?

Collaborative Issues	Step 25	Step 29
If staff from a third party is partly or completely responsible for this area:		
The organization's requirements for monitoring physical security are formally communicated to all contractors and service providers that monitor physical access to the building and premises, work areas, IT hardware, and software media.	❑ Current	❑ Change
The organization's requirements for monitoring physical security are informally communicated to all contractors and service providers that monitor physical access to the building and premises, work areas, IT hardware, and software media.	❑ Current	❑ Change
The organization's requirements for monitoring physical security are not communicated to all contractors and service providers that monitor physical access to the building and premises, work areas, IT hardware, and software media.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

Step 25: To what extent does your organization verify that this third party is addressing requirements in this area?

Step 29: Will any mitigation activities change how you verify that this third party is addressing requirements in this area? Do you want to make any additional changes to how you verify that requirements are being met?

Verification	Step 25	Step 29
If staff from a third party is partly or completely responsible for this area:		
The organization formally verifies that contractors and service providers have met the requirements for monitoring physical security.	❑ Current	❑ Change
The organization informally verifies that contractors and service providers have met the requirements for monitoring physical security.	❑ Current	❑ Change
The organization does not verify that contractors and service providers have met the requirements for monitoring physical security.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

9. System and Network Management

Stoplight Status ☐

Step 25: Who is currently responsible for system and network management?

Step 29: Will any mitigation activities change responsibility for system and network management? Do you want to make any additional changes affecting responsibility for system and network management?

Responsibility	Step 25			Step 29		
	☐ Current			☐ Change		
Task	Internal	External	Combined	Internal	External	Combined
Configuring IT hardware and software	☐	☐	☐	☐	☐	☐
Securely storing sensitive information (e.g., backups stored off site, process for discarding sensitive information)	☐	☐	☐	☐	☐	☐
Checking the integrity of installed software	☐	☐	☐	☐	☐	☐
Keeping systems up to date with respect to revisions, patches, and recommendations in security advisories	☐	☐	☐	☐	☐	☐
Making and tracking changes to IT hardware and software	☐	☐	☐	☐	☐	☐
Managing passwords, accounts, and privileges	☐	☐	☐	☐	☐	☐
Selecting system and network management tools	☐	☐	☐	☐	☐	☐
_____	☐	☐	☐	☐	☐	☐
_____	☐	☐	☐	☐	☐	☐
_____	☐	☐	☐	☐	☐	☐

9. System and Network Management

Step 25: To what extent are procedures for this area formally documented?

Step 29: Will any mitigation activities change the extent to which procedures are formally documented for this area?
Do you want to make any additional changes to how procedures are documented for this area?

Procedures	Step 25	Step 29
If staff from your organization is partly or completely responsible for this area:		
The organization has formally documented system and network management procedures.	❑ Current	❑ Change
The organization has some formally documented system and network management procedures. Some procedures in this area are informal and undocumented.	❑ Current	❑ Change
The organization has informal and undocumented system and network management procedures.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

Step 25: To what extent are staff members required to attend training in this area?

Step 29: Will any mitigation activities change the requirement for attending training in this area?
Do you want to make any additional changes to the requirement for attending training in this area?

Training	Step 25	Step 29
If staff from your organization is partly or completely responsible for this area:		
Information technology staff members are required to attend training for managing systems and networks and using system and network management tools.	❑ Current	❑ Change
Information technology staff members can attend training for managing systems and networks and using system and network management tools if they request it.	❑ Current	❑ Change
The organization generally does not provide opportunities for information technology staff members to attend training for managing systems and networks and using system and network management tools. Information technology staff members learn about system and network management on their own.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

9. System and Network Management

Stoplight Status ☐

Third Party A:_____

Step 25: To what extent does your organization formally communicate its requirements in this area to this third party?

Step 29: Will any mitigation activities change how your organization communicates its requirements to this third party? Do you want to make any additional changes to how you communicate requirements to this third party?

Collaborative Issues	Step 25	Step 29
If staff from a third party is partly or completely responsible for this area:		
The organization's security-related system and network management requirements are formally communicated to all contractors and service providers that maintain systems and networks.	☐ Current	☐ Change
The organization's security-related system and network management requirements are informally communicated to all contractors and service providers that maintain systems and networks.	☐ Current	☐ Change
The organization's security-related system and network management requirements are not communicated to all contractors and service providers that maintain systems and networks.	☐ Current	☐ Change
_____	☐ Current	☐ Change
_____		

Step 25: To what extent does your organization verify that this third party is addressing requirements in this area?

Step 29: Will any mitigation activities change how you verify that this third party is addressing requirements in this area? Do you want to make any additional changes to how you verify that requirements are being met?

Verification	Step 25	Step 29
If staff from a third party is partly or completely responsible for this area:		
The organization formally verifies that contractors and service providers have met the requirements for security-related system and network management.	☐ Current	☐ Change
The organization informally verifies that contractors and service providers have met the requirements for security-related system and network management.	☐ Current	☐ Change
The organization does not verify that contractors and service providers have met the requirements for security-related system and network management.	☐ Current	☐ Change
_____	☐ Current	☐ Change
_____		

9. System and Network Management

Third Party B:_____

Step 25: To what extent does your organization formally communicate its requirements in this area to this third party?

Step 29: Will any mitigation activities change how your organization communicates its requirements to this third party? Do you want to make any additional changes to how you communicate requirements to this third party?

Collaborative Issues	Step 25	Step 29
If staff from a third party is partly or completely responsible for this area:		
The organization's security-related system and network management requirements are formally communicated to all contractors and service providers that maintain systems and networks.	❑ Current	❑ Change
The organization's security-related system and network management requirements are informally communicated to all contractors and service providers that maintain systems and networks.	❑ Current	❑ Change
The organization's security-related system and network management requirements are not communicated to all contractors and service providers that maintain systems and networks.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

Step 25: To what extent does your organization verify that this third party is addressing requirements in this area?

Step 29: Will any mitigation activities change how you verify that this third party is addressing requirements in this area? Do you want to make any additional changes to how you verify that requirements are being met?

Verification	Step 25	Step 29
If staff from a third party is partly or completely responsible for this area:		
The organization formally verifies that contractors and service providers have met the requirements for security-related system and network management.	❑ Current	❑ Change
The organization informally verifies that contractors and service providers have met the requirements for security-related system and network management.	❑ Current	❑ Change
The organization does not verify that contractors and service providers have met the requirements for security-related system and network management.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

10. Monitoring and Auditing IT Security

Stoplight Status ☐

Step 25: Who is currently responsible for monitoring and auditing IT security?

Step 29: Will any mitigation activities change responsibility for monitoring and auditing IT security? Do you want to make any additional changes affecting responsibility for monitoring and auditing IT security?

Responsibility	**Step 25**			**Step 29**		
	☐ Current			☐ Change		
Task	Internal	External	Combined	Internal	External	Combined
Using system and network monitoring tools to track system and network activity	☐	☐	☐	☐	☐	☐
Auditing the firewall and other security components periodically for compliance with policy	☐	☐	☐	☐	☐	☐
Investigating and addressing any unusual activity that is identified	☐	☐	☐	☐	☐	☐
_____	☐	☐	☐	☐	☐	☐
_____	☐	☐	☐	☐	☐	☐
_____	☐	☐	☐	☐	☐	☐
_____	☐	☐	☐	☐	☐	☐
_____	☐	☐	☐	☐	☐	☐
_____	☐	☐	☐	☐	☐	☐
_____	☐	☐	☐	☐	☐	☐

10. Monitoring and Auditing IT Security

Step 25: To what extent are procedures for this area formally documented?

Step 29: Will any mitigation activities change the extent to which procedures are formally documented for this area? Do you want to make any additional changes to how procedures are documented for this area?

Procedures	Step 25	Step 29
If staff from your organization is partly or completely responsible for this area:		
The organization has formally documented procedures for monitoring network-based access to systems and networks.	❑ Current	❑ Change
The organization has some formally documented procedures for monitoring network-based access to systems and networks. Some procedures in this area are informal and undocumented.	❑ Current	❑ Change
The organization has informal and undocumented procedures for monitoring network-based access to systems and networks.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

Step 25: To what extent are staff members required to attend training in this area?

Step 29: Will any mitigation activities change the requirement for attending training in this area? Do you want to make any additional changes to the requirement for attending training in this area?

Training	Step 25	Step 29
If staff from your organization is partly or completely responsible for this area:		
Information technology staff members are required to attend training for monitoring network-based access to systems and networks and using monitoring and auditing tools.	❑ Current	❑ Change
Information technology staff members can attend training for monitoring network-based access to systems and networks and using monitoring and auditing tools if they request it.	❑ Current	❑ Change
The organization generally does not provide opportunities for information technology staff members to attend training for monitoring network-based access to systems and networks and using monitoring and auditing tools. Information technology staff members learn about monitoring systems and networks on their own.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

10. Monitoring and Auditing IT Security

Stoplight Status ☐

Third Party A:_____

Step 25: To what extent does your organization formally communicate its requirements in this area to this third party?

Step 29: Will any mitigation activities change how your organization communicates its requirements to this third party? Do you want to make any additional changes to how you communicate requirements to this third party?

Collaborative Issues	Step 25	Step 29
If staff from a third party is partly or completely responsible for this area:		
The organization's requirements for monitoring information technology security are formally communicated to all contractors and service providers that monitor systems and networks.	☐ Current	☐ Change
The organization's requirements for monitoring information technology security are informally communicated to all contractors and service providers that monitor systems and networks.	☐ Current	☐ Change
The organization's requirements for monitoring information technology security are not communicated to all contractors and service providers that monitor systems and networks.	☐ Current	☐ Change
_____	☐ Current	☐ Change
_____		

Step 25: To what extent does your organization verify that this third party is addressing requirements in this area?

Step 29: Will any mitigation activities change how you verify that this third party is addressing requirements in this area? Do you want to make any additional changes to how you verify that requirements are being met?

Verification	Step 25	Step 29
If staff from a third party is partly or completely responsible for this area:		
The organization formally verifies that contractors and service providers have met the requirements for monitoring information technology security.	☐ Current	☐ Change
The organization informally verifies that contractors and service providers have met the requirements for monitoring information technology security.	☐ Current	☐ Change
The organization does not verify that contractors and service providers have met the requirements for monitoring information technology security.	☐ Current	☐ Change
_____	☐ Current	☐ Change
_____		

10. Monitoring and Auditing IT Security

Third Party B:_____

Step 25: To what extent does your organization formally communicate its requirements in this area to this third party?

Step 29: Will any mitigation activities change how your organization communicates its requirements to this third party? Do you want to make any additional changes to how you communicate requirements to this third party?

Collaborative Issues	Step 25	Step 29
If staff from a third party is partly or completely responsible for this area:		
The organization's requirements for monitoring information technology security are formally communicated to all contractors and service providers that monitor systems and networks.	❑ Current	❑ Change
The organization's requirements for monitoring information technology security are informally communicated to all contractors and service providers that monitor systems and networks.	❑ Current	❑ Change
The organization's requirements for monitoring information technology security are not communicated to all contractors and service providers that monitor systems and networks.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

Step 25: To what extent does your organization verify that this third party is addressing requirements in this area?

Step 29: Will any mitigation activities change how you verify that this third party is addressing requirements in this area? Do you want to make any additional changes to how you verify that requirements are being met?

Verification	Step 25	Step 29
If staff from a third party is partly or completely responsible for this area:		
The organization formally verifies that contractors and service providers have met the requirements for monitoring information technology security.	❑ Current	❑ Change
The organization informally verifies that contractors and service providers have met the requirements for monitoring information technology security.	❑ Current	❑ Change
The organization does not verify that contractors and service providers have met the requirements for monitoring information technology security.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

11. Authentication and Authorization

Stoplight Status ☐

Step 25: Who is currently responsible for authentication and authorization?

Step 29: Will any mitigation activities change responsibility for authentication and authorization?
Do you want to make any additional changes affecting responsibility for authentication and authorization?

Responsibility	**Step 25**			**Step 29**		
	☐ Current			☐ Change		
Task	Internal	External	Combined	Internal	External	Combined
Implementing access controls (e.g., file permissions, network configuration) to restrict user access to information, sensitive systems, specific applications and services, and network connections	☐	☐	☐	☐	☐	☐
Implementing user authentication (e.g., passwords, biometrics) to restrict user access to information, sensitive systems, specific applications and services, and network connections	☐	☐	☐	☐	☐	☐
Establishing and terminating access to systems and information for both individuals and groups	☐	☐	☐	☐	☐	☐
_____	☐	☐	☐	☐	☐	☐
_____	☐	☐	☐	☐	☐	☐
_____	☐	☐	☐	☐	☐	☐
_____	☐	☐	☐	☐	☐	☐
_____	☐	☐	☐	☐	☐	☐
_____	☐	☐	☐	☐	☐	☐
_____	☐	☐	☐	☐	☐	☐

11. Authentication and Authorization

Step 25: To what extent are procedures for this area formally documented?

Step 29: Will any mitigation activities change the extent to which procedures are formally documented for this area? Do you want to make any additional changes to how procedures are documented for this area?

Procedures	Step 25	Step 29
If staff from your organization is partly or completely responsible for this area:		
The organization has formally documented authorization and authentication procedures for restricting user access to information, sensitive systems, specific applications and services, and network connections.	❑ Current	❑ Change
The organization has some formally documented authorization and authentication procedures for restricting user access to information, sensitive systems, specific applications and services, and network connections. Some procedures in this area are informal and undocumented.	❑ Current	❑ Change
The organization has informal and undocumented authorization and authentication procedures for restricting user access to information, sensitive systems, specific applications and services, and network connections.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

Step 25: To what extent are staff members required to attend training in this area?

Step 29: Will any mitigation activities change the requirement for attending training in this area? Do you want to make any additional changes to the requirement for attending training in this area?

Training	Step 25	Step 29
If staff from your organization is partly or completely responsible for this area:		
Information technology staff members are required to attend training for implementing technological measures to restrict user access to information, sensitive systems, specific applications and services, and network connections.	❑ Current	❑ Change
Information technology staff members can attend training for implementing technological measures to restrict user access to information, sensitive systems, specific applications and services, and network connections if they request it.	❑ Current	❑ Change
The organization generally does not provide opportunities for information technology staff members to attend training for implementing technological measures to restrict user access to information, sensitive systems, specific applications and services, and network connections. Information technology staff members learn about authentication and authorization on their own.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

11. Authentication and Authorization

Stoplight Status ☐

Third Party A:_____

Step 25: To what extent does your organization formally communicate its requirements in this area to this third party?

Step 29: Will any mitigation activities change how your organization communicates its requirements to this third party? Do you want to make any additional changes to how you communicate requirements to this third party?

Collaborative Issues	Step 25	Step 29
If staff from a third party is partly or completely responsible for this area:		
The organization's requirements for controlling access to systems and information are formally communicated to all contractors and service providers that provide authentication and authorization services.	☐ Current	☐ Change
The organization's requirements for controlling access to systems and information are informally communicated to all contractors and service providers that monitor systems and networks.	☐ Current	☐ Change
The organization's requirements for controlling access to systems and information are not communicated to all contractors and service providers that monitor systems and networks.	☐ Current	☐ Change
_____	☐ Current	☐ Change
_____		

Step 25: To what extent does your organization verify that this third party is addressing requirements in this area?

Step 29: Will any mitigation activities change how you verify that this third party is addressing requirements in this area? Do you want to make any additional changes to how you verify that requirements are being met?

Verification	Step 25	Step 29
If staff from a third party is partly or completely responsible for this area:		
The organization formally verifies that contractors and service providers have met the requirements for authentication and authorization.	☐ Current	☐ Change
The organization informally verifies that contractors and service providers have met the requirements for authentication and authorization.	☐ Current	☐ Change
The organization does not verify that contractors and service providers have met the requirements for authentication and authorization.	☐ Current	☐ Change
_____	☐ Current	☐ Change
_____		

11. Authentication and Authorization

Third Party B:_____

Step 25: To what extent does your organization formally communicate its requirements in this area to this third party?

Step 29: Will any mitigation activities change how your organization communicates its requirements to this third party? Do you want to make any additional changes to how you communicate requirements to this third party?

Collaborative Issues	Step 25	Step 29
If staff from a third party is partly or completely responsible for this area:		
The organization's requirements for controlling access to systems and information are formally communicated to all contractors and service providers that provide authentication and authorization services.	❑ Current	❑ Change
The organization's requirements for controlling access to systems and information are informally communicated to all contractors and service providers that monitor systems and networks.	❑ Current	❑ Change
The organization's requirements for controlling access to systems and information are not communicated to all contractors and service providers that monitor systems and networks.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

Step 25: To what extent does your organization verify that this third party is addressing requirements in this area?

Step 29: Will any mitigation activities change how you verify that this third party is addressing requirements in this area? Do you want to make any additional changes to how you verify that requirements are being met?

Verification	Step 25	Step 29
If staff from a third party is partly or completely responsible for this area:		
The organization formally verifies that contractors and service providers have met the requirements for authentication and authorization.	❑ Current	❑ Change
The organization informally verifies that contractors and service providers have met the requirements for authentication and authorization.	❑ Current	❑ Change
The organization does not verify that contractors and service providers have met the requirements for authentication and authorization.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

12. Vulnerability Management

Stoplight Status ☐

Step 25: Who is currently responsible for vulnerability management?

Step 29: Will any mitigation activities change responsibility for vulnerability management?
Do you want to make any additional changes affecting responsibility for vulnerability management?

Responsibility	Step 25			Step 29		
	☐ Current			☐ Change		
Task	Internal	External	Combined	Internal	External	Combined
Selecting vulnerability evaluation tools, checklists, and scripts	☐	☐	☐	☐	☐	☐
Scheduling and performing technology vulnerability evaluations on a periodic basis	☐	☐	☐	☐	☐	☐
Keeping up to date with known vulnerability types and attack methods	☐	☐	☐	☐	☐	☐
Reviewing sources of information on vulnerability announcements, security alerts, and notices	☐	☐	☐	☐	☐	☐
Interpreting the results of technology vulnerability evaluations	☐	☐	☐	☐	☐	☐
Addressing technology vulnerabilities that are identified	☐	☐	☐	☐	☐	☐
Maintaining secure storage and disposition of technology vulnerability data	☐	☐	☐	☐	☐	☐
_____	☐	☐	☐	☐	☐	☐
_____	☐	☐	☐	☐	☐	☐
_____	☐	☐	☐	☐	☐	☐

12. Vulnerability Management

Step 25: To what extent are procedures for this area formally documented?

Step 29: Will any mitigation activities change the extent to which procedures are formally documented for this area? Do you want to make any additional changes to how procedures are documented for this area?

Procedures	Step 25	Step 29
If staff from your organization is partly or completely responsible for this area:		
The organization has formally documented vulnerability management procedures.	❑ Current	❑ Change
The organization has some formally documented vulnerability management procedures. Some procedures in this area are informal and undocumented.	❑ Current	❑ Change
The organization has informal and undocumented vulnerability management procedures.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

Step 25: To what extent are staff members required to attend training in this area?

Step 29: Will any mitigation activities change the requirement for attending training in this area? Do you want to make any additional changes to the requirement for attending training in this area?

Training	Step 25	Step 29
If staff from your organization is partly or completely responsible for this area:		
Information technology staff members are required to attend training for managing technology vulnerabilities and using vulnerability evaluation tools.	❑ Current	❑ Change
Information technology staff members can attend training for managing technology vulnerabilities and using vulnerability evaluation tools if they request it.	❑ Current	❑ Change
The organization generally does not provide opportunities for information technology staff members to attend training for managing technology vulnerabilities and using vulnerability evaluation tools. Information technology staff members learn about vulnerability management on their own.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

12. Vulnerability Management

Stoplight Status ☐

Third Party A:_____

Step 25: To what extent does your organization formally communicate its requirements in this area to this third party?

Step 29: Will any mitigation activities change how your organization communicates its requirements to this third party? Do you want to make any additional changes to how you communicate requirements to this third party?

Collaborative Issues	Step 25	Step 29
If staff from a third party is partly or completely responsible for this area:		
The organization's vulnerability management requirements are formally communicated to all contractors and service providers that manage technology vulnerabilities.	☐ Current	☐ Change
The organization's vulnerability management requirements are informally communicated to all contractors and service providers that manage technology vulnerabilities.	☐ Current	☐ Change
The organization's vulnerability management requirements are not communicated to all contractors and service providers that manage technology vulnerabilities.	☐ Current	☐ Change
_____	☐ Current	☐ Change
_____		

Step 25: To what extent does your organization verify that this third party is addressing requirements in this area?

Step 29: Will any mitigation activities change how you verify that this third party is addressing requirements in this area? Do you want to make any additional changes to how you verify that requirements are being met?

Verification	Step 25	Step 29
If staff from a third party is partly or completely responsible for this area:		
The organization formally verifies that contractors and service providers have met the requirements for vulnerability management.	☐ Current	☐ Change
The organization informally verifies that contractors and service providers have met the requirements for vulnerability management.	☐ Current	☐ Change
The organization does not verify that contractors and service providers have met the requirements for vulnerability management.	☐ Current	☐ Change
_____	☐ Current	☐ Change
_____		

12. Vulnerability Management

Third Party B:_____

Step 25: To what extent does your organization formally communicate its requirements in this area to this third party?

Step 29: Will any mitigation activities change how your organization communicates its requirements to this third party? Do you want to make any additional changes to how you communicate requirements to this third party?

Collaborative Issues	Step 25	Step 29
If staff from a third party is partly or completely responsible for this area:		
The organization's vulnerability management requirements are formally communicated to all contractors and service providers that manage technology vulnerabilities.	❑ Current	❑ Change
The organization's vulnerability management requirements are informally communicated to all contractors and service providers that manage technology vulnerabilities.	❑ Current	❑ Change
The organization's vulnerability management requirements are not communicated to all contractors and service providers that manage technology vulnerabilities.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

Step 25: To what extent does your organization verify that this third party is addressing requirements in this area?

Step 29: Will any mitigation activities change how you verify that this third party is addressing requirements in this area? Do you want to make any additional changes to how you verify that requirements are being met?

Verification	Step 25	Step 29
If staff from a third party is partly or completely responsible for this area:		
The organization formally verifies that contractors and service providers have met the requirements for vulnerability management.	❑ Current	❑ Change
The organization informally verifies that contractors and service providers have met the requirements for vulnerability management.	❑ Current	❑ Change
The organization does not verify that contractors and service providers have met the requirements for vulnerability management.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

13. Encryption

Stoplight Status ☐

Step 25: Who is currently responsible for encryption?
Step 29: Will any mitigation activities change responsibility for encryption?
Do you want to make any additional changes affecting responsibility for encryption?

Responsibility	Step 25			Step 29		
	☐ Current			☐ Change		
Task	Internal	External	Combined	Internal	External	Combined
Implementing encryption technologies to protect sensitive information that is electronically stored and transmitted (e.g., data encryption, public key infrastructure, virtual private network technology)	☐	☐	☐	☐	☐	☐
Implementing encrypted protocols for remotely managing systems, routers, and firewalls	☐	☐	☐	☐	☐	☐
_____	☐	☐	☐	☐	☐	☐
_____	☐	☐	☐	☐	☐	☐
_____	☐	☐	☐	☐	☐	☐
_____	☐	☐	☐	☐	☐	☐
_____	☐	☐	☐	☐	☐	☐

Step 25: To what extent are procedures for this area formally documented?
Step 29: Will any mitigation activities change the extent to which procedures are formally documented for this area?
Do you want to make any additional changes to how procedures are documented for this area?

Procedures	Step 25	Step 29
If staff from your organization is partly or completely responsible for this area:		
The organization has formally documented procedures for implementing and using encryption technologies.	☐ Current	☐ Change
The organization has some formally documented procedures for implementing and using encryption technologies. Some procedures in this area are informal and undocumented.	☐ Current	☐ Change
The organization has informal and undocumented procedures for implementing and using encryption technologies.	☐ Current	☐ Change
_____ _____	☐ Current	☐ Change

13. Encryption

Step 25: To what extent are IT staff members required to attend training in this area?

Step 29: Will any mitigation activities change the requirement for attending training in this area?
Do you want to make any additional changes to the requirement for attending training in this area?

Information Technology Staff Training	Step 25	Step 29
If staff from your organization is partly or completely responsible for this area:		
Information technology staff members are required to attend training for implementing encryption technologies.	❑ Current	❑ Change
Information technology staff members can attend training for implementing encryption technologies if they request it.	❑ Current	❑ Change
The organization generally does not provide opportunities for information technology staff members to attend training for implementing encryption technologies. Information technology staff members learn about implementing encryption technologies on their own.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

Step 25: To what extent are staff members required to attend training in this area?

Step 29: Will any mitigation activities change the requirement for attending training in this area?
Do you want to make any additional changes to the requirement for attending training in this area?

Staff Training	Step 25	Step 29
All staff members are required to attend training for using encryption technologies.	❑ Current	❑ Current
All staff members can attend training for using encryption technologies if they request it.	❑ Current	❑ Current
The organization generally does not provide opportunities for staff members to attend training for using encryption technologies. Staff members learn about using encryption technologies on their own.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

13. Encryption

Stoplight Status ☐

Third Party A:_____

Step 25: To what extent does your organization formally communicate its requirements in this area to this third party?

Step 29: Will any mitigation activities change how your organization communicates its requirements to this third party? Do you want to make any additional changes to how you communicate requirements to this third party?

Collaborative Issues	Step 25	Step 29
If staff from a third party is partly or completely responsible for this area:		
The organization's requirements for protecting sensitive information are formally communicated to all contractors and service providers that provide encryption technologies.	☐ Current	☐ Change
The organization's requirements for protecting sensitive information are informally communicated to all contractors and service providers that provide encryption technologies.	☐ Current	☐ Change
The organization's requirements for protecting sensitive information are not communicated to all contractors and service providers that provide encryption technologies.	☐ Current	☐ Change
_____	☐ Current	☐ Change
_____		

Step 25: To what extent does your organization verify that this third party is addressing requirements in this area?

Step 29: Will any mitigation activities change how you verify that this third party is addressing requirements in this area? Do you want to make any additional changes to how you verify that requirements are being met?

Verification	Step 25	Step 29
If staff from a third party is partly or completely responsible for this area:		
The organization formally verifies that contractors and service providers have met the requirements for implementing encryption technologies.	☐ Current	☐ Change
The organization informally verifies that contractors and service providers have met the requirements for implementing encryption technologies.	☐ Current	☐ Change
The organization does not verify that contractors and service providers have met the requirements for implementing encryption technologies.	☐ Current	☐ Change
_____	☐ Current	☐ Change
_____		

13. Encryption

Third Party B:_____

Step 25: To what extent does your organization formally communicate its requirements in this area to this third party?

Step 29: Will any mitigation activities change how your organization communicates its requirements to this third party? Do you want to make any additional changes to how you communicate requirements to this third party?

Collaborative Issues	Step 25	Step 29
If staff from a third party is partly or completely responsible for this area:		
The organization's requirements for protecting sensitive information are formally communicated to all contractors and service providers that provide encryption technologies.	❑ Current	❑ Change
The organization's requirements for protecting sensitive information are informally communicated to all contractors and service providers that provide encryption technologies.	❑ Current	❑ Change
The organization's requirements for protecting sensitive information are not communicated to all contractors and service providers that provide encryption technologies.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

Step 25: To what extent does your organization verify that this third party is addressing requirements in this area?

Step 29: Will any mitigation activities change how you verify that this third party is addressing requirements in this area? Do you want to make any additional changes to how you verify that requirements are being met?

Verification	Step 25	Step 29
If staff from a third party is partly or completely responsible for this area:		
The organization formally verifies that contractors and service providers have met the requirements for implementing encryption technologies.	❑ Current	❑ Change
The organization informally verifies that contractors and service providers have met the requirements for implementing encryption technologies.	❑ Current	❑ Change
The organization does not verify that contractors and service providers have met the requirements for implementing encryption technologies.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

14. Security Architecture and Design

Stoplight Status ☐

Step 25: Who is currently responsible for security architecture and design?

Step 29: Will any mitigation activities change responsibility for security architecture and design?
Do you want to make any additional changes affecting responsibility for security architecture and design?

Responsibility	**Step 25**			**Step 29**		
	☐ Current			☐ Change		
Task	Internal	External	Combined	Internal	External	Combined
Designing security controls in new and revised systems and networks	☐	☐	☐	☐	☐	☐
Documenting and revising diagrams that show the enterprise-wide security architecture and network topology	☐	☐	☐	☐	☐	☐
_____	☐	☐	☐	☐	☐	☐
_____	☐	☐	☐	☐	☐	☐
_____	☐	☐	☐	☐	☐	☐
_____	☐	☐	☐	☐	☐	☐
_____	☐	☐	☐	☐	☐	☐
_____	☐	☐	☐	☐	☐	☐
_____	☐	☐	☐	☐	☐	☐
_____	☐	☐	☐	☐	☐	☐

14. Security Architecture and Design

Step 25: To what extent are practices for this area formally documented?

Step 29: Will any mitigation activities change the extent to which practices are formally documented for this area? Do you want to make any additional changes to how practices are documented for this area?

Procedures	Step 25	Step 29
If staff from your organization is partly or completely responsible for this area:		
The organization has formally documented security architecture and design practices.	❑ Current	❑ Change
The organization has some formally documented security architecture and design practices. Some practices in this area are informal and undocumented.	❑ Current	❑ Change
The organization has informal and undocumented security architecture and design practices.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

Step 25: To what extent are staff members required to attend training in this area?

Step 29: Will any mitigation activities change the requirement for attending training in this area? Do you want to make any additional changes to the requirement for attending training in this area?

Training	Step 25	Step 29
If staff from your organization is partly or completely responsible for this area:		
Staff members are required to attend training for designing secure systems and networks.	❑ Current	❑ Change
Staff members can attend training for designing secure systems and networks if they request it.	❑ Current	❑ Change
The organization generally does not provide opportunities for staff members to attend training for designing secure systems and networks. Staff members learn about security architecture and design on their own.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

14. Security Architecture and Design

Stoplight Status ☐

Third Party A:_____

Step 25: To what extent does your organization formally communicate its requirements in this area to this third party?

Step 29: Will any mitigation activities change how your organization communicates its requirements to this third party? Do you want to make any additional changes to how you communicate requirements to this third party?

Collaborative Issues	Step 25	Step 29
If staff from a third party is partly or completely responsible for this area:		
The organization's security-related requirements are formally communicated to all contractors and service providers that design systems and networks.	☐ Current	☐ Change
The organization's security-related requirements are informally communicated to all contractors and service providers that design systems and networks.	☐ Current	☐ Change
The organization's security-related requirements are not communicated to all contractors and service providers that design systems and networks.	☐ Current	☐ Change
_____	☐ Current	☐ Change
_____		

Step 25: To what extent does your organization verify that this third party is addressing requirements in this area?

Step 29: Will any mitigation activities change how you verify that this third party is addressing requirements in this area? Do you want to make any additional changes to how you verify that requirements are being met?

Verification	Step 25	Step 29
If staff from a third party is partly or completely responsible for this area:		
The organization formally verifies that contractors and service providers have met the requirements for security architecture and design.	☐ Current	☐ Change
The organization informally verifies that contractors and service providers have met the requirements for security architecture and design.	☐ Current	☐ Change
The organization does not verify that contractors and service providers have met the requirements for security architecture and design.	☐ Current	☐ Change
_____	☐ Current	☐ Change
_____		

14. Security Architecture and Design

Third Party B:_____

Step 25: To what extent does your organization formally communicate its requirements in this area to this third party?

Step 29: Will any mitigation activities change how your organization communicates its requirements to this third party? Do you want to make any additional changes to how you communicate requirements to this third party?

Collaborative Issues	Step 25	Step 29
If staff from a third party is partly or completely responsible for this area:		
The organization's security-related requirements are formally communicated to all contractors and service providers that design systems and networks.	❑ Current	❑ Change
The organization's security-related requirements are informally communicated to all contractors and service providers that design systems and networks.	❑ Current	❑ Change
The organization's security-related requirements are not communicated to all contractors and service providers that design systems and networks.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

Step 25: To what extent does your organization verify that this third party is addressing requirements in this area?

Step 29: Will any mitigation activities change how you verify that this third party is addressing requirements in this area? Do you want to make any additional changes to how you verify that requirements are being met?

Verification	Step 25	Step 29
If staff from a third party is partly or completely responsible for this area:		
The organization formally verifies that contractors and service providers have met the requirements for security architecture and design.	❑ Current	❑ Change
The organization informally verifies that contractors and service providers have met the requirements for security architecture and design.	❑ Current	❑ Change
The organization does not verify that contractors and service providers have met the requirements for security architecture and design.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

15. Incident Management

Stoplight Status ☐

Step 25: Who is currently responsible for incident management?

Step 29: Will any mitigation activities change responsibility for incident management?
Do you want to make any additional changes affecting responsibility for incident management?

Responsibility	Step 25			Step 29		
	☐ Current			☐ Change		
Task	Internal	External	Combined	Internal	External	Combined
Documenting and revising procedures for identifying, reporting, and responding to suspected security incidents and violations	☐	☐	☐	☐	☐	☐
Documenting and revising policies and procedures for working with law enforcement agencies	☐	☐	☐	☐	☐	☐
Testing incident management procedures on a periodic basis	☐	☐	☐	☐	☐	☐
_____	☐	☐	☐	☐	☐	☐
_____	☐	☐	☐	☐	☐	☐
_____	☐	☐	☐	☐	☐	☐
_____	☐	☐	☐	☐	☐	☐
_____	☐	☐	☐	☐	☐	☐
_____	☐	☐	☐	☐	☐	☐
_____	☐	☐	☐	☐	☐	☐

15. Incident Management

Step 25: To what extent are procedures for this area formally documented?

Step 29: Will any mitigation activities change the extent to which procedures are formally documented for this area? Do you want to make any additional changes to how procedures are documented for this area?

Procedures	Step 25	Step 29
If staff from your organization is partly or completely responsible for this area:		
The organization has formally documented incident management procedures.	❑ Current	❑ Change
The organization has some formally documented incident management procedures. Some procedures in this area are informal and undocumented.	❑ Current	❑ Change
The organization has informal and undocumented incident management procedures.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

Step 25: To what extent are staff members required to attend training in this area?

Step 29: Will any mitigation activities change the requirement for attending training in this area? Do you want to make any additional changes to the requirement for attending training in this area?

Training	Step 25	Step 29
If staff from your organization is partly or completely responsible for this area:		
Designated staff members are required to attend training for incident management.	❑ Current	❑ Change
Designated staff members can attend training for incident management if they request it.	❑ Current	❑ Change
The organization generally does not provide opportunities for designated staff members to attend training for incident management. Designated staff members learn about incident management on their own.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

15. Incident Management

Stoplight Status ☐

Third Party A:_____

Step 25: To what extent does your organization formally communicate its requirements in this area to this third party?

Step 29: Will any mitigation activities change how your organization communicates its requirements to this third party? Do you want to make any additional changes to how you communicate requirements to this third party?

Collaborative Issues	Step 25	Step 29
If staff from a third party is partly or completely responsible for this area:		
The organization's requirements for managing incidents are formally communicated to all contractors and service providers that provide incident management services.	☐ Current	☐ Change
The organization's requirements for managing incidents are informally communicated to all contractors and service providers that provide incident management services.	☐ Current	☐ Change
The organization's requirements for managing incidents are not communicated to all contractors and service providers that provide incident management services.	☐ Current	☐ Change
_____	☐ Current	☐ Change
_____		

Step 25: To what extent does your organization verify that this third party is addressing requirements in this area?

Step 29: Will any mitigation activities change how you verify that this third party is addressing requirements in this area? Do you want to make any additional changes to how you verify that requirements are being met?

Verification	Step 25	Step 29
If staff from a third party is partly or completely responsible for this area:		
The organization formally verifies that contractors and service providers have met the requirements for managing incidents.	☐ Current	☐ Change
The organization informally verifies that contractors and service providers have met the requirements for managing incidents.	☐ Current	☐ Change
The organization does not verify that contractors and service providers have met the requirements for managing incidents.	☐ Current	☐ Change
_____	☐ Current	☐ Change
_____		

15. Incident Management

Third Party B:_____

Step 25: To what extent does your organization formally communicate its requirements in this area to this third party?

Step 29: Will any mitigation activities change how your organization communicates its requirements to this third party? Do you want to make any additional changes to how you communicate requirements to this third party?

Collaborative Issues	Step 25	Step 29
If staff from a third party is partly or completely responsible for this area:		
The organization's requirements for managing incidents are formally communicated to all contractors and service providers that provide incident management services.	❑ Current	❑ Change
The organization's requirements for managing incidents are informally communicated to all contractors and service providers that provide incident management services.	❑ Current	❑ Change
The organization's requirements for managing incidents are not communicated to all contractors and service providers that provide incident management services.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

Step 25: To what extent does your organization verify that this third party is addressing requirements in this area?

Step 29: Will any mitigation activities change how you verify that this third party is addressing requirements in this area? Do you want to make any additional changes to how you verify that requirements are being met?

Verification	Step 25	Step 29
If staff from a third party is partly or completely responsible for this area:		
The organization formally verifies that contractors and service providers have met the requirements for managing incidents.	❑ Current	❑ Change
The organization informally verifies that contractors and service providers have met the requirements for managing incidents.	❑ Current	❑ Change
The organization does not verify that contractors and service providers have met the requirements for managing incidents.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

5 Mitigation Activities Guide

Phase 3
Process S5
Activity S5.3

Mitigation Activities Guide	The *Mitigation Activities Guide* describes potential mitigation activities for each security practice area. You will find examples of mitigation activities related to each security practice area in this guide.

1. Security Awareness and Training	Candidate Mitigation Activities
Mitigation Activity	**Protection Strategy Link**
Develop and document a training strategy that includes security awareness training and security-related training for supported technologies.	Training Strategy
Provide periodic security awareness training for *all* employees on a periodic basis (e.g., _____time(s) every _____ years).	Security Awareness Training
Provide security awareness training for *new* staff members as part of their orientation activities.	Security Awareness Training
Require IT staff members to attend security-related training for any technologies that they support.	Security-Related Training for Supported Technologies
Enable IT staff members to attend security-related training for any technologies that they support.	Security-Related Training for Supported Technologies
Implement a *formal* mechanism for providing staff members with periodic updates/bulletins about important security issues.	Periodic Security Updates
Implement an *informal* mechanism for providing staff members with periodic updates/bulletins about important security issues.	Periodic Security Updates
Implement a *formal* mechanism for tracking and verifying that staff members receive appropriate security-related training.	Training Verification
Implement an *informal* mechanism for tracking and verifying that staff members receive appropriate security-related training.	Training Verification
Schedule a one-time offering of security awareness training.	---
Send selected staff members to training for a specific technology (i.e., a limited or one-time offering in a specific technology).	---
Cross train selected staff members to use specific information systems and/or applications. Cross-trained staff members will back up the primary users of those systems and/or applications.	---
Cross train selected staff members to provide specific skills or services. Cross-trained staff members will back up the staff members who normally provide those skills or services.	---
Cross train selected IT staff members to configure and maintain specific information systems, networks, and/or applications. Cross-trained IT staff members will back up the primary administrators who normally maintain those systems, networks, and/or applications.	---
Ensure that selected staff members understand how to notify and work with third parties that own or operate key systems. These people will be able to work with third parties when there are problems with systems owned and/or operated by those third parties.	---

2. Security Strategy	Candidate Mitigation Activities
Mitigation Activity	**Protection Strategy Link**
Implement a *formal* mechanism for integrating • security considerations into business strategies • business strategies and goals into security strategies and policies	Business and Security Strategy Integration
Implement an *informal* mechanism for integrating • security considerations into business strategies • business strategies and goals into security strategies and policies	Business and Security Strategy Integration
Document security strategies, goals, and objectives for *all* aspects of information security.	Documented Strategies
Document the security strategies, goals, and objectives for *selected* security-related areas.	Documented Strategies
Incorporate information about the organization's security strategy into the organization's security-awareness training program.	Staff Awareness

3. Security Management	Candidate Mitigation Activities
Mitigation Activity	**Protection Strategy Link**
Document information security roles and responsibilities for *all* staff in the organization.	Roles and Responsibilities
Document information security roles and responsibilities for *selected* staff members.	Roles and Responsibilities
Include a separate line item for information security activities in the *organization's budget.*	Funding
Include a separate line item for information security activities in organization's *information technology budget.*	Funding
Use the results of an information security risk evaluation to determine the level of funding for information security activities.	Funding
Document procedures for including security considerations in the organization's hiring and termination processes.	Human Resource Procedures
Document a process for *assessing and managing* the organization's information security risks.	Risk Management
Document a process for *assessing* the organization's information security risks.	Risk Management
Incorporate information about the organization's security management process into the organization's security-awareness training program.	Staff Awareness
Implement a *formal* mechanism for providing managers with summaries of important security-related information.	Management Awareness
Implement an *informal* mechanism for providing managers with summaries of important security-related information.	Management Awareness

4. Security Policies and Regulations — **Candidate Mitigation Activities**

Mitigation Activity	Protection Strategy Link
Document a *comprehensive* set of security-related policies.	Documented Policies
Document security-related policies for *selected areas*.	Documented Policies
Implement a formal mechanism for *creating and updating* security-related policies.	Policy Management
Implement a formal mechanism for *creating* security-related policies.	Policy Management
Implement formal procedures for enforcing security-related policies.	Policy Enforcement
Incorporate information about the organization's security policies and regulations into the organization's security-awareness training program.	Staff Awareness
Document procedures for complying with *all* information security policies, applicable laws and regulations, and insurance requirements.	Policy and Regulation Compliance
Document procedures for complying with *selected* security policies, applicable laws and regulations, and insurance requirements.	Policy and Regulation Compliance

5. Collaborative Security Management	Candidate Mitigation Activities
Mitigation Activity	**Protection Strategy Link**
Document policies and procedures for protecting information when working with collaborators and partners.	Collaborators and Partners
Document policies and procedures for protecting information when working with contractors and subcontractors.	Contractors and Subcontractors
Document policies and procedures for protecting information when working with service providers.	Service Providers
Implement a *formal* mechanism (e.g., contract mechanism) for communicating information protection requirements to all appropriate third parties.	Requirements
Implement an *informal* mechanism (e.g., assign responsibility) for communicating information protection requirements to all appropriate third parties.	Requirements
Implement a *formal* mechanism (e.g., contract mechanism) for verifying that all third-party organizations, outsourced security services, mechanisms, and technologies meet the organization's information protection requirements.	Verification
Implement an *informal* mechanism (e.g., assign responsibility) for verifying that all third-party organizations, outsourced security services, mechanisms, and technologies meet the organization's information protection requirements.	Verification
Incorporate information about the organization's policies and procedures for collaborative security management into the organization's security-awareness training program.	Staff Awareness

6. Contingency Planning/Disaster Recovery	Candidate Mitigation Activities
Mitigation Activity	**Protection Strategy Link**
Perform an analysis defining the criticality of *all* operations, applications, and data.	Business Operations Analysis
Perform an analysis defining the criticality of *selected* operations, applications, and/or data.	Business Operations Analysis
Document business continuity or emergency operation plans, disaster recovery plan(s), and contingency plan(s) for responding to emergencies.	Documented Plans
Document *a subset of the following plans* for responding to emergencies: business continuity or emergency operation plans, disaster recovery plan(s), and contingency plan(s).	Documented Plans
Formally test the organization's business continuity or emergency operation plans, disaster recovery plan(s), and contingency plan(s) for responding to emergencies.	Tested Plans
Formally test a *subset of the following plans* for responding to emergencies: business continuity or emergency operation plans, disaster recovery plan(s), and contingency plan(s).	Tested Plans
Incorporate contingency plans into the organization's disaster recovery and business continuity plans for accessing critical information.	Information Access
Incorporate information about the organization's contingency, disaster recovery, and business continuity plans into the organization's security-awareness training program.	Staff Awareness
Document a disaster recovery plan for a specific system maintained by the information technology staff.	---
Develop a disaster recovery plan for a specific system maintained by a third party.	---
Document a business continuity plan for specific business processes.	---
Purchase insurance for any security problems related to a specific system.	---
Configure and maintain a hot backup for a system.	---
Configure and maintain a cold backup for a specific system.	---

7. Physical Access Control	Candidate Mitigation Activities
Mitigation Activity	**Protection Strategy Link**
Change responsibility for controlling physical access to the building and premises (e.g., controlling visitor access).	Responsibility
Change responsibility for controlling physical access to work areas (e.g., controlling staff and visitor access).	Responsibility
Change responsibility for controlling physical access to IT hardware.	Responsibility
Change responsibility for controlling physical access to software media.	Responsibility
Document formal procedures for controlling physical access to the building and premises, work areas, IT hardware, and software media.	Procedures
Send selected staff members to training for controlling physical access to the building and premises, work areas, IT hardware, and software media.	Training
Implement a *formal* mechanism (e.g., contract mechanism) for communicating the organization's requirements for physical access control to all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.	Collaborative Issues
Implement an *informal* mechanism (e.g., assign responsibility) for communicating the organization's requirements for physical access control to all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.	Collaborative Issues
Implement a *formal* mechanism (e.g., contract mechanism) for verifying that the organization's requirements for physical access control have been met by all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.	Verification
Implement an *informal* mechanism (e.g., assign responsibility) for verifying that the organization's requirements for physical access control have been met by all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.	Verification

Candidate Mitigation Activities	7. Physical Access Control
Mitigation Activity	**Protection Strategy Link**
Develop procedures for controlling physical access to • the building and premises • selected work areas • IT hardware • software media • other	---
Rearrange office/work spaces to restrict physical access to systems, computers, or other devices by unauthorized personnel.	---
Implement sign-in sheets to manage visitors' access to the building and/or designated work areas.	---
Implement card access to restrict physical access to the building.	---
Implement card access to restrict physical access to specific work areas.	---
Replace door locks in specific work areas.	---
Retain the services of security guards to protect the premises.	---
Rearrange the physical setup of computing equipment in specific areas to counteract environmental threats.	---
Perform an audit of physical security to identify security weaknesses in the physical infrastructure.	---
Develop procedures for specific systems defining the designated time that a device can remain logged on before that device is automatically locked or logged off.	---
Arrange a meeting with all appropriate contractors, service providers, and third parties to communicate requirements for controlling physical access in the organization and to verify that those requirements have been met.	---

8. Monitoring and Auditing Physical Security	Candidate Mitigation Activities
Mitigation Activity	**Protection Strategy Link**
Change responsibility for keeping maintenance records that document repairs and modifications to IT hardware.	Responsibility
Change responsibility for monitoring physical access to controlled IT hardware	Responsibility
Change responsibility for monitoring physical access to controlled IT software media.	Responsibility
Change responsibility for monitoring physical access to restricted work areas.	Responsibility
Change responsibility for reviewing monitoring records on a periodic basis.	Responsibility
Change responsibility for investigating and addressing any unusual activity that is identified.	Responsibility
Document formal procedures for monitoring physical access to the building and premises, work areas, IT hardware, and software media.	Procedures
Send selected staff members to training for monitoring physical access to the building and premises, work areas, IT hardware, and software media.	Training
Implement a *formal* mechanism (e.g., contract mechanism) for communicating the organization's requirements for monitoring physical security to all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.	Collaborative Issues
Implement an *informal* mechanism (e.g., assign responsibility) for communicating the organization's requirements for monitoring physical security to all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.	Collaborative Issues
Implement a *formal* mechanism (e.g., contract mechanism) for verifying that the organization's requirements for monitoring physical security have been met by all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.	Verification
Implement an *informal* mechanism (e.g., assign responsibility) for verifying that the organization's requirements for monitoring physical security have been met by all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.	Verification

Candidate Mitigation Activities	8. Monitoring and Auditing Physical Security
Mitigation Activity	**Protection Strategy Link**
Install video cameras in designated areas of the premises.	---
Retain the services of security guards to monitor activity on the premises.	---
Implement sign-in sheets to log visitors' access to the building and/or designated work areas.	---
Implement card access to log physical access to the building and/or designated work areas.	---
Arrange a meeting with all appropriate contractors, service providers, and third parties to communicate requirements for monitoring physical security in the organization and to verify that those requirements have been met.	---

9. System and Network Management	Candidate Mitigation Activities
Mitigation Activity	**Protection Strategy Link**
Change responsibility for configuring IT hardware and software.	Responsibility
Change responsibility for securely storing sensitive information (e.g., backups stored off site, process for discarding sensitive information).	Responsibility
Change responsibility for checking the integrity of installed software.	Responsibility
Change responsibility for keeping systems up to date with respect to revisions, patches, and recommendations in security advisories.	Responsibility
Change responsibility for making and tracking changes to IT hardware and software.	Responsibility
Change responsibility for managing passwords, accounts, and privileges.	Responsibility
Change responsibility for selecting system and network management tools.	Responsibility
Document formal procedures for managing systems and networks.	Procedures
Send selected staff members to training for managing systems and networks.	Training
Implement a *formal* mechanism (e.g., contract mechanism) for communicating the organization's requirements for secure system and network management to all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.	Collaborative Issues
Implement an *informal* mechanism (e.g., assign responsibility) for communicating the organization's requirements for secure system and network management to all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.	Collaborative Issues
Implement a *formal* mechanism (e.g., contract mechanism) for verifying that the organization's requirements for secure system and network management have been met by all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.	Verification
Implement an *informal* mechanism (e.g., assign responsibility) for verifying that the organization's requirements for secure system and network management have been met by all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.	Verification

Candidate Mitigation Activities	9. System and Network Management
Mitigation Activity	**Protection Strategy Link**
Check the configuration of IT hardware and software on specific systems.	---
Check the integrity of installed software on specific systems.	---
Check specific systems to ensure that they are up to date with respect to revisions, patches, and recommendations in security advisories.	---
Check specific systems for default accounts and accounts that are no longer used.	---
Check specific systems for easy-to-crack passwords.	---
Check specific systems to see if they are running unnecessary services.	---
Check specific systems for the presence of viruses or other malicious code.	---
Arrange a meeting with all appropriate contractors, service providers, and third parties to communicate requirements for securely managing systems and networks in the organization and to verify that those requirements have been met.	---

10. Monitoring and Auditing IT Security	Candidate Mitigation Activities
Mitigation Activity	**Protection Strategy Link**
Change responsibility for using system and network monitoring tools to track system and network activity.	Responsibility
Change responsibility for periodically auditing the firewall and other security components for compliance with policy.	Responsibility
Change responsibility for investigating and addressing any unusual activity that is identified.	Responsibility
Document formal procedures for monitoring network access to systems and networks.	Procedures
Send selected staff members to training for monitoring network access to systems and networks.	Training
Implement a *formal* mechanism (e.g., contract mechanism) for communicating the organization's requirements for monitoring IT security to all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.	Collaborative Issues
Implement an *informal* mechanism (e.g., assign responsibility) for communicating the organization's requirements for monitoring IT security to all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.	Collaborative Issues
Implement a *formal* mechanism (e.g., contract mechanism) for verifying that the organization's requirements for monitoring IT security have been met by all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.	Verification
Implement an *informal* mechanism (e.g., assign responsibility) for verifying that the organization's requirements for monitoring IT security have been met by all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.	Verification

Candidate Mitigation Activities	10. Monitoring and Auditing IT Security
Mitigation Activity	**Protection Strategy Link**
Develop procedures for • reviewing system logs • using system and network monitoring tools to track system activity • auditing the firewall and other security components periodically for compliance with policy • investigating and addressing any unusual activity that is identified	---
Implement an intrusion detection system and assign an IT staff member the responsibility of tracking network activity.	---
Perform an audit of the firewall and other security components to ensure that they are compliant with the organization's security policies.	---
Arrange a meeting with all appropriate contractors, service providers, and third parties to communicate requirements for monitoring IT security in the organization and to verify that those requirements have been met.	---

11. Authentication and Authorization — **Candidate Mitigation Activities**

Mitigation Activity	Protection Strategy Link
Change responsibility for implementing access controls (e.g., file permissions, network configuration) to restrict user access to information, sensitive systems, specific applications and services, and network connections.	Responsibility
Change responsibility for implementing user authentication (e.g., passwords, biometrics) to restrict user access to information, sensitive systems, specific applications and services, and network connections.	Responsibility
Change responsibility for establishing and terminating access to systems and information for both individuals and groups.	Responsibility
Document formal procedures for restricting user access to information, sensitive systems, specific applications and services, and network connections.	Procedures
Send selected staff members to training for implementing technological measures to restrict user access to information, sensitive systems, specific applications and services, and network connections.	Training
Implement a *formal* mechanism (e.g., contract mechanism) for communicating the organization's requirements for controlling access to systems and information to all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.	Collaborative Issues
Implement an *informal* mechanism (e.g., assign responsibility) for communicating the organization's requirements for controlling access to systems and information to all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.	Collaborative Issues
Implement a *formal* mechanism (e.g., contract mechanism) for verifying that the organization's requirements for controlling access to systems and information have been met by all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.	Verification
Implement an *informal* mechanism (e.g., assign responsibility) for verifying that the organization's requirements for controlling access to systems and information have been met by all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.	Verification

Candidate Mitigation Activities	11. Authentication and Authorization
Mitigation Activity	**Protection Strategy Link**
Check access controls (e.g., file permissions, network configuration) on specific systems.	---
Check that appropriate authentication mechanisms (e.g., passwords, biometrics) are used to restrict user access to specific systems.	---
Check specific systems for easy-to-crack passwords.	---
Check specific systems to ensure that all devices that access those systems automatically timeout after a designated period of time.	---
Arrange a meeting with all appropriate contractors, service providers, and third parties to communicate requirements for controlling access to systems and information in the organization and to verify that those requirements have been met.	---

12. Vulnerability Management	Candidate Mitigation Activities
Mitigation Activity	**Protection Strategy Link**
Change responsibility for selecting vulnerability evaluation tools, checklists, and scripts.	Responsibility
Change responsibility for scheduling and performing technology vulnerability evaluations on a periodic basis.	Responsibility
Change responsibility for keeping up to date with known vulnerability types and attack methods.	Responsibility
Change responsibility for reviewing sources of information on vulnerability announcements, security alerts, and notices.	Responsibility
Change responsibility for interpreting the results of technology vulnerability evaluations.	Responsibility
Change responsibility for addressing technology vulnerabilities that are identified.	Responsibility
Change responsibility for maintaining secure storage and disposition of technology vulnerability data.	Responsibility
Document formal procedures for managing technology vulnerabilities.	Procedures
Send selected staff members to training for managing technology vulnerabilities.	Training
Implement a *formal* mechanism (e.g., contract mechanism) for communicating the organization's requirements for managing technology vulnerabilities to all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.	Collaborative Issues
Implement an *informal* mechanism (e.g., assign responsibility) for communicating the organization's requirements for managing technology vulnerabilities to all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.	Collaborative Issues
Implement a *formal* mechanism (e.g., contract mechanism) for verifying that the organization's requirements for managing technology vulnerabilities have been met by all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.	Verification
Implement an *informal* mechanism (e.g., assign responsibility) for verifying that the organization's requirements for managing technology vulnerabilities have been met by all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.	Verification

Candidate Mitigation Activities	12. Vulnerability Management
Mitigation Activity	**Protection Strategy Link**
Check specific systems for technology vulnerabilities.	---
Perform an audit of information technology security to identify security weaknesses in the computing infrastructure.	---
Contract with an outside organization to attack your organization's systems and network via the Internet (i.e., penetration testing, red team).	---
Arrange a meeting with all appropriate contractors, service providers, and third parties to communicate requirements for managing technology vulnerabilities in the organization and to verify that those requirements have been met.	---

13. Encryption	Candidate Mitigation Activities
Mitigation Activity	**Protection Strategy Link**
Change responsibility for implementing encryption technologies to protect sensitive information that is electronically stored and transmitted (e.g., data encryption, public key infrastructure, virtual private network technology).	Responsibility
Change responsibility for implementing encrypted protocols for remotely managing systems, routers, and firewalls.	Responsibility
Change responsibility for implementing encrypted protocols for remotely managing systems, routers, and firewalls.	Responsibility
Document formal procedures for implementing and using encryption technologies.	Procedures
Send selected IT staff members to training for implementing encryption technologies.	Information Technology Staff Training
Send selected staff members to training for using encryption technologies.	Staff Training
Implement a *formal* mechanism (e.g., contract mechanism) for communicating the organization's requirements for protecting sensitive information to all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.	Collaborative Issues
Implement an *informal* mechanism (e.g., assign responsibility) for communicating the organization's requirements for protecting sensitive information to all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.	Collaborative Issues
Implement a *formal* mechanism (e.g., contract mechanism) for verifying that the organization's requirements for protecting sensitive information have been met by all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.	Verification
Implement an *informal* mechanism (e.g., assign responsibility) for verifying that the organization's requirements for protecting sensitive information have been met by all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.	Verification

Candidate Mitigation Activities	13. Encryption
Mitigation Activity	**Protection Strategy Link**
Implement encryption technologies to protect specific types of information and/or systems.	---
Arrange a meeting with all appropriate contractors, service providers, and third parties to communicate requirements for protecting sensitive information in the organization and to verify that those requirements have been met.	---

14. Security Architecture and Design	Candidate Mitigation Activities
Mitigation Activity	**Protection Strategy Link**
Change responsibility for designing security controls in new and revised systems and networks.	Responsibility
Change responsibility for documenting and revising diagrams that show the enterprise-wide security architecture and network topology.	Responsibility
Document formal security architecture and design practices.	Procedures
Send selected staff members to training for designing secure systems and networks.	Training
Implement a *formal* mechanism (e.g., contract mechanism) for communicating the organization's requirements for incorporating appropriate security features into systems and networks to all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.	Collaborative Issues
Implement an *informal* mechanism (e.g., assign responsibility) for communicating the organization's requirements for incorporating appropriate security features into systems and networks to all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.	Collaborative Issues
Implement a *formal* mechanism (e.g., contract mechanism) for verifying that the organization's requirements for incorporating appropriate security features into systems and networks have been met by all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.	Verification
Implement an *informal* mechanism (e.g., assign responsibility) for verifying that the organization's requirements for incorporating appropriate security features into systems and networks have been met by all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.	Verification

Candidate Mitigation Activities	14. Security Architecture and Design
Mitigation Activity	**Protection Strategy Link**
Update the design of specific systems to include appropriate security controls.	---
Investigate periodic crashes of specific systems and correct any design problems that lead to those crashes.	---
Document or update diagrams that show the enterprise-wide security architecture and network topology.	---
Arrange a meeting with all appropriate contractors, service providers, and third parties to communicate requirements for incorporating appropriate security features into systems and networks and to verify that those requirements have been met.	---

15. Incident Management	Candidate Mitigation Activities
Mitigation Activity	**Protection Strategy Link**
Change responsibility for documenting and revising procedures for identifying, reporting, and responding to suspected security incidents and violations.	Responsibility
Change responsibility for documenting and revising policies and procedures for working with law enforcement agencies.	Responsibility
Change responsibility for testing incident management procedures on a periodic basis.	Responsibility
Document formal procedures for managing incidents.	Procedures
Send selected staff members to training for managing incidents.	Training
Implement a *formal* mechanism (e.g., contract mechanism) for communicating the organization's requirements for managing incidents to all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.	Collaborative Issues
Implement an *informal* mechanism (e.g., assign responsibility) for communicating the organization's requirements for managing incidents to all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.	Collaborative Issues
Implement a *formal* mechanism (e.g., contract mechanism) for verifying that the organization's requirements for managing incidents have been met by all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.	Verification
Implement an *informal* mechanism (e.g., assign responsibility) for verifying that the organization's requirements for managing incidents have been met by all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.	Verification

Candidate Mitigation Activities	15. Incident Management
Mitigation Activity	**Protection Strategy Link**
Test current incident management procedures.	---
Arrange a meeting with all appropriate contractors, service providers, and third parties to communicate requirements for managing incidents in the organization and to verify that those requirements have been met.	---

6 Mitigation Plan Worksheet

	Phase 3 Process S5 Activity S5.3
Step 28	Develop mitigation plans for each security practice area selected during Step 27. As you complete this step, if you have difficulty coming up with potential mitigation activities for a security practice area, review examples of mitigation activities for that area in the *Mitigation Activities Guide*.

Mitigation Area: _____

Step 28

Mitigation Activity	Rationale
Which mitigation activities are you going to implement in this security practice area?	*Why did you select each activity?*

Mitigation Responsibility	**Additional Support**
Who needs to be involved in implementing each activity? Why?	*What additional support will be needed when implementing each activity (e.g., funding, commitment of staff, sponsorship)?*

Mitigation Area: _____

Step 28

Mitigation Activity	Rationale
Which mitigation activities are you going to implement in this security practice area?	*Why did you select each activity?*

Mitigation Responsibility	**Additional Support**
Who needs to be involved in implementing each activity? Why?	*What additional support will be needed when implementing each activity (e.g., funding, commitment of staff, sponsorship)?*

Mitigation Area: _____

Step 28

Mitigation Activity	Rationale
Which mitigation activities are you going to implement in this security practice area?	*Why did you select each activity?*

Mitigation Responsibility	**Additional Support**
Who needs to be involved in implementing each activity? Why?	*What additional support will be needed when implementing each activity (e.g., funding, commitment of staff, sponsorship)?*

Mitigation Area: _____

Step 28

Mitigation Activity	Rationale
Which mitigation activities are you going to implement in this security practice area?	*Why did you select each activity?*

Mitigation Responsibility	**Additional Support**
Who needs to be involved in implementing each activity? Why?	*What additional support will be needed when implementing each activity (e.g., funding, commitment of staff, sponsorship)?*

Mitigation Area: _____

Step 28

Mitigation Activity	Rationale
Which mitigation activities are you going to implement in this security practice area?	*Why did you select each activity?*

Mitigation Responsibility	**Additional Support**
Who needs to be involved in implementing each activity? Why?	*What additional support will be needed when implementing each activity (e.g., funding, commitment of staff, sponsorship)?*

Mitigation Area: _____

Step 28

Mitigation Activity	Rationale
Which mitigation activities are you going to implement in this security practice area?	*Why did you select each activity?*

Mitigation Responsibility	**Additional Support**
Who needs to be involved in implementing each activity? Why?	*What additional support will be needed when implementing each activity (e.g., funding, commitment of staff, sponsorship)?*

7 Next Steps Worksheet

	Phase 3 Process S5 Activity S5.5
Step 30	Determine what your organization must do to implement the results of this evaluation and improve its security posture.

Step 30

Management Sponsorship for Security Improvement

What must management do to support the implementation of OCTAVE-S results?

Consider the following:

- Contribute funds to information security activities.
- Assign staff to information security activities.
- Ensure that staff members have sufficient time allocated to information security activities.
- Enable staff to receive training about information security.
- Make information security a strategic priority.

Monitoring Implementation
What will the organization do to track progress and ensure that the results of this evaluation are implemented?

Expanding the Current Information Security Risk Evaluation
Will you expand the current OCTAVE-S evaluation to include additional critical assets? Which ones?

Next Information Security Risk Evaluation
When will the organization conduct its next OCTAVE-S evaluation?

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
(Leave Blank)	January 2005	Final

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
OCTAVE-S Implementation Guide, Version 1.0, Volume 9	F19628-00-C-0003

6. AUTHOR(S)

Christopher Alberts, Audrey Dorofee, James Stevens, Carol Woody

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	CMU/SEI-2003-HB-003

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSORING/MONITORING AGENCY REPORT NUMBER
HQ ESC/XPK 5 Eglin Street Hanscom AFB, MA 01731-2116	

11. SUPPLEMENTARY NOTES

12A DISTRIBUTION/AVAILABILITY STATEMENT	12B DISTRIBUTION CODE
Unclassified/Unlimited, DTIC, NTIS	

13. ABSTRACT (MAXIMUM 200 WORDS)

The Operationally Critical Threat, Asset, and Vulnerability Evaluation℠ (OCTAVE®) approach defines a risk-based strategic assessment and planning technique for security. OCTAVE is a self-directed approach, meaning that people from an organization assume responsibility for setting the organization's security strategy. OCTAVE-S is a variation of the approach tailored to the limited means and unique constraints typically found in small organizations (less than 100 people). OCTAVE-S is led by a small, interdisciplinary team (three to five people) of an organization's personnel who gather and analyze information, producing a protection strategy and mitigation plans based on the organization's unique operational security risks. To conduct OCTAVE-S effectively, the team must have broad knowledge of the organization's business and security processes, so it will be able to conduct all activities by itself.

14. SUBJECT TERMS	15. NUMBER OF PAGES
information security, risk management, OCTAVE	132

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL